RICKERT.LAW

Rickert Rechtsanwaltsgesellschaft mbH · Colmantstraße 15 · 53115 Bonn

Landgericht Hamburg
Sievekingplatz 1
20355 Hamburg

Ihr Zeichen:	310 O 99/21	Sachbearbeiter:	RA Thomas Rickert
Unser Zeichen:	[redacted]	E-Mail:	kanzlei@rickert.net

per beA

Bonn, den 31.08.2021

In dem einstweiligen Verfügungsverfahren

[redacted]

./. Quad9 Stiftung

310 O 99/21

wird namens und in Vollmacht der Antragsgegnerin

Rickert Rechtsanwaltsgesellschaft mbH

Rechtsanwälte
Thomas Rickert[1]
Patrick Jardin[2]
Carsten Toß[2]
Roman Wagner[4]
Jan Lutterbach[2]
Matthias Bendixen[3]
Nicolas Golliart[3]
Lena Wassermann[3]
Christian Kirchberger[3]
Sandra Schulte[3]
Jasmin Eul[3]

Kanzlei
Colmantstraße 15
53115 Bonn
Tel.: +49.228.74 898.0
Fax: +49.228.74 898.66
www.rickert.law

HRB 9269
AG Bonn

Geschäftskonto
Commerzbank AG
IBAN: DE81 3804 0007 0241 4480 00
BIC: C0BADEFF380

Deutsche Bank AG
IBAN: DE20 3807 0059 0053 1012 00
BIC: DEUTDEDK380

Anderkonto
Commerzbank AG
IBAN: DE55 3804 0007 0241 4480 80
BIC: COBADEFF380

[1]Geschäftsführender Gesellschafter
[2]Senior Associate Partner
[3]Associate Partner
[4]Of Counsel

Widerspruch

gegen die durch den Beschluss vom 12.05.2021 erlassene einstweilige Verfügung eingelegt.

Es wird beantragt,

> die einstweilige Verfügung aufzuheben und den zugrundeliegenden Antrag zurückzuweisen.

Weiter wird beantragt,

> die Vollziehung der einstweiligen Verfügung ohne Sicherheitsleistung einzustellen.

Begründung

Das mit der Beschlussverfügung angeordnete Verbot besteht zu Unrecht. Die Antragstellerin haftet nicht als Störerin. Sie wurde nicht auf einen konkreten Rechtsverstoß hingewiesen. Selbst, wenn ein ordnungsgemäßer Hinweis ergangen wäre, besteht keine Störerhaftung der Antragsgegnerin wegen ihrer Privilegierung nach TMG, da sie keinen adäquat-kausalen Beitrag zur öffentlichen Zugänglichmachung des Musikalbums [redacted] geleistet hat, sowie der Unverhältnismäßigkeit ihrer Inanspruchnahme. Die einstweilige Verfügung ist aufzuheben.

I. Sachverhalt

1. Keine Aktivlegitimation / Keine Nutzungsrechte der Antragstellerin

Der Geschäftssitz der Antragstellerin ist in München. Die Antragstellerin behauptet, sie sei Inhaberin der (ausschließlichen) Nutzungsrechte in Bezug auf das Musikalbum [redacted]

Die Antragstellerin macht ihre Aktivlegitimation nicht glaubhaft. Insbesondere legt sie keine schriftlichen Nachweise vor, aus denen sich ergibt, dass ihr die ausschließlichen Nutzungsrechte an den verfahrensgegenständlichen Werken und das Recht zur Rechtsverfolgung eingeräumt werden.

Es wird insofern bestritten, dass die Antragstellerin als Inhaberin der ausschließlichen Nutzungsrechte im Sinne des § 31 UrhG in Bezug auf das Album [redacted] der Musikgruppe [redacted] aktivlegitimiert ist. Die Antragstellerin legt nicht dar, welche Nutzungsrechte an dem genannten Werk sie innehabe.

2. Zur Antragsgegnerin

2.1. Gemeinnützige Stiftung

Die Antragsgegnerin ist eine gemeinnützige Stiftung nach Schweizer Recht, die sich mit Spendengeldern finanziert und keine kommerziellen Zwecke verfolgt.

Glaubhaftmachung: Internetauszug des Handelsregisteramtes des Kantons Zürich, als **Anlage AG 1**.

Hinsichtlich der Reputation der Antragsgegnerin sei erwähnt, dass etwa die City of London Police den Einsatz des Dienstes der Antragsgegnerin empfiehlt und dessen Vorteile und Nutzung erörtert.

Glaubhaftmachung: Screenshot der Veröffentlichung der City of London Police unter http://news.cityoflondon.police.uk/r/945/ibm_packet_clearing_house_and_global_cyber_allia, eine Übersetzung kann im Bedarfsfall nachgereicht werden, als **Anlage AG 2**.

2.2. Technischer Dienst

2.2.1 DNS-Service der Antragsgegnerin

Die Antragsgegnerin betreibt als unabhängiger DNS-Dienst so genannte rekursive Resolver. Sie erbringt ihren Dienst ausschließlich im Interesse der Öffentlichkeit ohne Gewinnerzielungsabsicht.

Ziel der Antragsgegnerin ist es dabei, alternativ zu den großen DNS-Anbietern einen kostenfreien Dienst zu erbringen, der den Datenschutz der Anfragenden in den Vordergrund stellt. Da bei jedem Besuch einer Website über die Eingabe des Uniform Resource Locators (URL) in den Browser eine Abfrage des angefragten Hosts über einen DNS-Resolver erfolgt, sind die dort anfallenden Daten einschließlich derer mit Personenbezug wirtschaftlich interessant und werden regelmäßig kommerzialisiert.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

Die Antragsgegnerin hingegen protokolliert keine Daten zu den Anfragenden und erstellt keine Profile der Anfragenden.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

Der Schutz der Anfragenden vor einer unerwünschten Erhebung und weiteren Verarbeitung ihrer Daten liegt somit im öffentlichen Interesse.

2.2.2 Domain Name System / Rekursive Resolver

Das Domain Name System (DNS) wird gemeinhin verglichen mit einem Telefonbuch, in dem Namen von Anschlussteilnehmern den jeweiligen Telefonnummern zugeordnet werden. Im DNS werden alphanumerische Domains sodann numerischen IP-Adressen zugeordnet.

Der Telefonbuchvergleich erklärt allerdings die Rolle des DNS-Dienstes der Antragsgegnerin nicht in Gänze. Man stelle sich dafür drei Personen vor, von denen die erste eine Telefonnummer wissen möchte („Anfragender"), die zweite auf halbem Weg zum Telefonbuch steht („rekursiver Resolver") und die dritte das Telefonbuch in Händen hält bzw. den Telefonbucheintrag verwaltet („autoritativer DNS-Server"). In diesem bildhaften Vergleich kommt der Antragsgegnerin die Rolle der zweiten Person zu, welche weder die erste noch die dritte Person kennt und mit dieser in Beziehung steht und zudem weder Einfluss darauf noch Wissen darüber hat, wer sich hinter der angefragten Telefonnummer verbirgt. Diese zweite Person gibt die fraglichen Informationen lediglich weiter. Die Antragsgegnerin verwaltet mithin nur die Anfragen. Der Inhalt, der sich hinter der Telefonnummer verbirgt, wird von der Antragsgegnerin weder verstanden noch analysiert.

Eine weitere Ergänzung des Telefonbuchvergleiches ist dahingehend erforderlich, dass es ein zentrales Telefonbuch nicht gibt, sondern ein Verzeichnisdienst darüber Auskunft gibt, wo ein Telefonbucheintrag zu finden ist. Im zweiten Schritt gleicht die Anfrage eher der Abfrage eines Telefonbuchverzeichnisses in Unternehmen, wo nicht für eine zentrale Telefonnummer, sondern gegebenenfalls Informationen über Tausende von Durchwahlen einzelner Anschlüsse, hinter denen Personen oder Geräte stehen, beauskunftet werden.

Eine weitere Besonderheit ist, dass einige „Telefonbuchbetreiber", also Betreiber autoritativer Nameserver, wünschen, dass ihre Information eine gewisse Zeit („Time to Live" oder „TTL") im Gedächtnis der zweiten Person bleibt, Anfragen also beantwortet werden können, ohne jedes Mal nachfragen zu müssen.

DNS-Anfragen können nunmehr auf zwei Arten beantwortet werden - autoritativ oder rekursiv.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

Bei der autoritativen Beantwortung von DNS-Anfragen werden die Informationen aus einer lokalen Zonendatei ermittelt, die vom Eigentümer der Zone festgelegt wurde und über die die autoritative Antwort erreicht wird.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

Die autoritative Beantwortung von DNS-Anfragen geschieht durch autoritative Nameserver, die die Quelle der Information dazu sind, wie DNS-Abfragen aufzulösen sind. Es sind also die autoritativen Nameserver, die Domains bzw. Hosts mit einer IP-Adresse verknüpfen. Es gibt

pro Domain lediglich eine primäre Quelle für den autoritativen Nameservereintrag und zumindest einen sekundären autoritativen Nameservereintrag. Wird der autoritative Nameservereintrag geändert oder gelöscht, so löst die betreffende Domain nicht mehr auf.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

Rekursive DNS-Resolver gibt es dagegen tausendfach. Nahezu jeder Access Provider betreibt gleichzeitig rekursive DNS-Resolver. In Deutschland sind dies etwa 800 Anbieter. Dazu kommt ein Mehrfaches dieser Zahl an nicht öffentlichen rekursiven DNS-Resolvern, die etwa in Unternehmensnetzen betrieben werden.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

Nach Auswertungen des Projekts Shadowserver (https://scan.shadowserver.org/dns/) wurden am 30.08.2021 in Deutschland 16.623 offene rekursive DNS-Resolver ermittelt.

Glaubhaftmachung: Kopie Ausdruck der Webseite, als **Anlage AG 5**.

Die Antragsgegnerin speichert aufgrund technischer Gegebenheiten die Anfrage so lange unverändert, wie die Time to Live und damit der Domaininhaber dies vorgibt. Eine längere oder auf anderem Wege durch die Antragsgegnerin konfigurierte Zwischenspeicherung erfolgt nicht. Mithin werden keine Inhalte zwischengespeichert, sondern nur die IP-Adresse für einen durch den autoritativen Nameserver vorgegebenen Zeitrahmen, damit bei der nächsten Anfrage der IP-Adresse der DNS-Resolver schneller antworten kann und das System entlastet wird.

Das vorbeschriebene DNS-Caching erfolgt in Übereinstimmung mit den „Request for Comments" (RFCs) 1034, 1035, 1123, 2181, 2308. Bei den RFCs handelt es sich um Dokumente, in denen die technischen Grundlagen des Internets beschrieben und definiert werden und die durch die IETF (Internet Engineering Task Force) verwaltet werden.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

2.2.3 Zusammenfassung: DNS-Dienst der Antragsgegnerin

Zusammenfassend ist festzuhalten, dass der automatisch ablaufende DNS-Dienst der Antragsgegnerin:

- keine autoritativen Informationen vorhält,
- lediglich DNS-Anfragen und Antworten an die jeweils andere Seite weitergibt und
- eine Zwischenspeicherung der Antworten lediglich den technischen Vorgaben entsprechend erfolgt.

2.3 Keine vertraglichen Beziehungen zwischen Anfragenden oder Domaininhaber und Antragsgegnerin

Sofern die Verwendung des Begriffes „Kunden" etwa auf S. 2 des Verfügungsbeschlusses vom 12.05.2021 darauf abstellen sollte, dass die Antragsgegnerin vertragliche Beziehungen zu den Anfragenden ihres Dienstes unterhält, ist dies nicht zutreffend. Über eine einfache Konfiguration in den Netzwerkeinstellungen können Anfragende den Dienst der Antragsgegnerin verwenden. Dies hängt nicht von der Zustimmung der Antragsgegnerin und auch nicht sonst von der Anerkennung von Vertragsbedingungen ab.

Tatsächlich kommt es auch vor, dass Anfragende den Dienst der Antragsgegnerin verwenden, ohne dies zu wissen, sofern dies von ihrem Netzwerkbetreiber voreingestellt ist. Es gibt aber auch viele Anfragende, die den Dienst der Antragsgegnerin bewusst wählen, um ihre Privatsphäre zu schützen und das Internet sicher zu nutzen.

Die Antragsgegnerin verfügt mithin über keine vertraglichen Beziehungen zu den Anfragenden oder den Access Providern. Dies gilt sowohl in Richtung der Betreiber von Diensten oder Inhalten, bezüglich derer DNS-Anfragen über das System der Antragsgegnerin aufgelöst werden, als auch im Hinblick auf Unternehmen oder Personen oder technische Infrastrukturen, die DNS-Abfragen auslösen.

2.4 Keine Sperrung der beanstandeten URIs möglich

Zunächst besitzt die Antragsgegnerin aufgrund der Natur des von ihr angebotenen Dienstes keine Möglichkeit, Kenntnis von den vorgehaltenen Diensten oder Inhalten unter einer Domain bzw. Third Level Domain (wie etwa abc.beispiel.de) oder Verzeichnissen (wie etwa beispiel.de/abc) zu erlangen.

Der automatisch ablaufende DNS-Dienst kann IP-Adressen für Domains abfragen und weitergeben, nicht aber für Verzeichnisse oder einzelne Elemente, d.h. „Uniform Resource Indicators" (URIs).

Eine Sperrung der beanstandeten URIs ist somit technisch nicht möglich.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

Technisch ist eine Sperrung lediglich auf Domainebene (etwa domain.de oder abc.domain.de) möglich. Dies bedeutet zwangsläufig, dass sämtliche URIs unter der betreffenden Domain mitgesperrt werden. Die Umsetzung der Anforderung der Beschlussverfügung ist nur über die vollständige Sperrung der Anfragen zu den Domains [redacted] bzw. [redacted] möglich.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

2.5 Auswirkungen des Blockens auf das System / Systemantworten

Die zur Umsetzung der Beschlussverfügung erforderliche technische Sperrung für Nutzer aus dem Gebiet der Bundesrepublik Deutschland ist im System der Antragsgegnerin technisch nicht vorgesehen.

Die zur Erfüllung der Anforderung der Beschlussverfügung erforderliche Sperrung der Anfragen zu den genannten Domains führt bei der betroffenen technischen Infrastruktur zudem zu erheblichem Ressourcenverbrauch, zu Leistungseinbußen der Systeme und zu längeren Antwortzeiten für alle Anfragen an die betroffenen Systeme.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

Im Zuge des Regelbetriebs werden häufig Prozessneustarts nötig, um einen Server bei Störungen wiederherzustellen. Bis der Neustart abgeschlossen ist, kann der jeweilige Server zwischen 12,5% und 33% des gesamten Datenverkehrs nicht bedienen ("Drop"). Bei einem repräsentativen Server mit Einsatz der umgesetzten Sperre erhöht sich die Zeit für die Validierung der Konfiguration und den Neustart des Prozesses durch die Einbeziehung der Blockierungstechnologie von 0,203 Sekunden auf 0,605 Sekunden. Dies führte zu einer Verdreifachung der abgebrochenen Anfragen während der Fehlerbehebung, was sich bei aktiven Servern negativ auf die Wahrnehmung der Zuverlässigkeit unseres Dienstes auswirken kann.

Während eines einstündigen vergleichenden Leistungstests führte die Deaktivierung der eigens angefertigten Blockierungsfunktion ohne einen Prozessneustart für einen einzelnen Server zu einem sofortigen Anstieg von durchschnittlich 2700 auf 3300 Antworten pro Sekunde. Gleichzeitig sank die CPU-Auslastung während des Testzeitraums um 10-15% im Vergleich zu einer entsprechenden Belastung in der Stunde zuvor. Dies zeigt, dass die Hinzufügung dieser Blockierungstechnik zu einer höheren Ressourcennutzung und einer geringeren Anzahl von Antworten pro Server führt, was bei hoher Last zu abgebrochenen Abfragen führen kann.

Um das System auf eine performante Umsetzung der gerichtlichen Anordnung umzustellen, müssten in etwa 6 Personenmonate an Entwicklungsaufwand betrieben werden und ein weiterer Entwickler und gegebenenfalls Systemadministrator eingestellt werden. Supportmitarbeiter müssen auf die neue Technologie geschult werden. Weiterhin müssten Prozesse und Standards eingeführt werden, die nicht technischer, sondern rechtlicher Natur sind.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

Die Umsetzung der Anordnung führt insofern in jeder Ausgestaltung zu einer erheblichen Belastung der Antragsgegnerin, die deren Existenz gefährdet.

Die Manipulation des Domain Name Systems, so dass DNS-Anfragen unzutreffend beantwortet werden, kann durch verschiedene technische Befehle („REFUSED", „SERVFAIL" oder „NXDOMAIN") erfolgen.

Grundsätzlich hat das Ausbleiben einer Antwort durch einen rekursiven Resolver, der lediglich Informationen von autoritativen DNS-Servern direkt oder über eine iterative Abfrage über weitere Resolver erhält und diese unverändert weitergibt, zur Folge, dass der Anfragende intransparent und unwissentlich zu einem anderen Resolver wechselt, der ihm eine Antwort gibt. Dies liegt in dem Umstand begründet, dass das DNS vorsieht, dass mindestens zwei Nameserver konfiguriert werden, um eine Beantwortung von DNS-Anfragen auch beim Ausfall eines der eingetragenen rekursiven DNS-Resolver zu gewährleisten.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

Die Antwort „REFUSED" würde dazu führen, dass Anfragende das System der Antragsgegnerin nicht weiter verwenden würden, da es eine Antwort verweigert. Diese technisch fragwürdige Umsetzung der gerichtlichen Anordnung würde unmittelbar den Betrieb und die Existenz der Antragsgegnerin gefährden.

Die Antragsgegnerin setzt den Tenor der einstweiligen Verfügung dadurch um, dass auf eine DNS-Anfrage nach der beanstandeten Domain mit „SERVFAIL" geantwortet wird. Damit wird auf eine DNS-Anfrage nicht mehr korrekt geantwortet mit der Folge, dass keine IP-Adressen mehr zurückgespielt werden.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

Typischerweise sind die anfragenden DNS-Resolver so konfiguriert, dass sie nach Erhalt einer „SERVFAIL"-Antwort dann nach einem DNS-Resolver suchen, der die konkrete Anfrage korrekt beantworten kann. Normalerweise wird die nächste Anfrage bei diesem Befehl dann allerdings wieder an die Infrastruktur der Antragsgegnerin gerichtet, so dass kein unmittelbarer Kundenverlust zu befürchten ist.

Schlussendlich wird die Abfrage damit allerdings nicht gänzlich blockiert, sondern an einen anderen rekursiven DNS-Resolver weitergegeben. Die Umsetzung der DNS-Sperre führt insofern dazu, dass Anfragende zu rekursiven DNS-Resolvern weitergeleitet werden, die den Malware-Schutz, der durch den Dienst der Antragsgegnerin besteht, nicht anbieten.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] als **Anlage AG 3**.

Eine dritte Option, die hier relevant ist, ist der Befehl „NXDOMAIN", wie er bei der Antragsgegnerin für die Malwarefilterung eingesetzt wird. Wenn der Client nach einem bösartigen Host fragt, verweigert der Resolver der Antragsgegnerin die Antwort mit der IP-Adresse mittels „NXDOMAIN" und verhindert so, dass sich der Client mit dem bösartigen Ziel verbindet. Die Anfrage wird damit abgeschlossen. Die Beantwortung von Anfragen mit

„NXDOMAIN" ist allerdings für die Beantwortung von Anfragen nach bösartigen Domains vorbehalten und kann nicht für die Blockierung etwa der streitgegenständlichen Domains eingesetzt werden.

Anfragende und Branchenexperten erwarten von der Antragsgegnerin, dass sie die DNS-Standards einhält, die in den derzeitigen Implementierungen keine Mechanismen zur Angabe des Grundes für eine bestimmte Antwort enthalten. Sie haben sich für die Verwendung von „SERVFAIL" ausgesprochen, um gefilterte bösartige Domains („NXDOMAIN", Autoritätsbit nicht gesetzt) nicht mit hier streitgegenständlichen Domains („SERVFAIL") zu verwechseln. Der Hauptunterschied zwischen den beiden Antworttypen besteht darin, dass die Anfragenden die Filterung bösartiger Domains verlangen, nicht aber eine solche Anforderung für zu sperrende Domains haben gemäß RFC 8914 4.17 und 4.18 (4.18 ist teilweise ein Beitrag der Antragsgegnerin, der in den RFC aufgenommen wurde) – ein Standard zur Filterung von Domains -, der aufgrund seiner Aktualität (23.10.2020) noch keine Übernahme oder Softwareimplementierung erfahren hat.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

Das Hinzufügen anderer Listeneinträge als derer zu schädigendem Code würde dazu führen, dass Anfragende befürchten müssten, dass Inhalte, die an ihrem Aufenthaltsort zulässig sind, nicht verfügbar sind. Würden insofern die zur Erhöhung der IT-Sicherheit eingesetzten Listen „verwässert", würde das Dienstmerkmal, den Schutz der Anfragenden zu erhöhen, erodiert. Die Folge wäre, dass der Dienst der Antragsgegnerin an Attraktivität verlöre und Kundenschwund zu erwarten wäre.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

2.6 Der Einsatz von Filterlisten (Filtering) ist nicht vergleichbar mit manueller Einrichtung einer DNS-Sperre (Blocking)

Die Antragstellerin hat vorgetragen, dass die Antragsgegnerin schon deshalb eine DNS-Sperre einrichten könne, weil sie Filterlisten von Quellen von Malware in ihr System einbinde. Die technischen und rechtlichen Implikationen sind dabei allerdings grundverschieden.

Die Antragsgegnerin bietet ihren Dienst, einschließlich des Malware-Schutzes, global einheitlich an. Zur Filterung bösartiger Domains setzt die Antragsgegnerin daher auch einheitliche Filterlisten ein, die dazu führen, dass die jeweiligen Domains weltweit für sämtliche Nutzer der Antragsgegnerin nicht erreichbar sind.

Auf globaler Ebene existieren verschiedene Organisationen, die Listen von Webseiten oder Servern führen und aktualisiert halten, von denen eine Bedrohung für die Sicherheit der Endgeräte der Anfragenden ausgeht, da dort schädigender Code vorgehalten wird. Es kann sich etwa um Quellen von Phishing, Botnets, Pharming oder Malware handeln. Die von der

Antragsgegnerin eingesetzten Listen werden von darauf spezialisierten Organisationen wie etwa abuse.ch oder auch von CERTs bereitgestellt.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

Gemein ist den von der Antragsgegnerin subskribierten und eingesetzten Listen, dass die dort geführten schädigenden Angebote global und ungeachtet einer bestimmten Jurisdiktion unerwünscht bzw. rechtswidrig sind. Zudem kann die Rechtswidrigkeit der Angebote aus sich heraus bestimmt werden. Der Einsatz von Filterlisten erfordert insofern keinerlei rechtliche Prüfkompetenz und keine personellen Ressourcen.

Die Antragsgegnerin prüft entgegen der Annahme in der Beschlussverfügung und dem Vortrag der Antragstellerin keines dieser Angebote, sondern setzt diese Listen ungeprüft ein. Es ist den Anfragenden überlassen, ob sie diesen die Netzwerksicherheit erhöhenden Dienst nutzen möchten oder nicht.

Die Antragsgegnerin hat allerdings die Möglichkeit, durch die Erstellung von Ausnahmeregeln Elemente aus der Liste zu entfernen, wenn sich ausnahmsweise ein Eintrag in die Filterliste als unberechtigt herausstellt. Damit wird die Erreichbarkeit unberechtigt gefilterter Angebote wieder hergestellt.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

Eine Beschränkung der Filterung von schädigenden Angeboten auf bestimmte Länder, auf bestimmte Nutzergruppen oder Regionen ist weder vorgesehen noch aufgrund der Natur der gelisteten Angebote erforderlich. Mit der weltweiten Gleichbehandlung von Listeneinträgen schädigender Angebote ist auch zu erklären, dass eine entsprechende Funktionalität, Listeneinträge pro Land zu differenzieren, im System der Antragsgegnerin nicht vorkommt. Die Umsetzung einer geografisch auf ein bestimmtes Territorium begrenzten DNS-Sperre ist durch die Aufnahme eines Eintrags in die Filterliste nicht möglich.

2.7 Kein hinreichender Hinweis der Antragstellerin auf Rechtsverletzung durch [redacted]

Weder das Hinweisschreiben des Verfahrensbevollmächtigten der Antragstellerin vom 23.03.2021 (Anlage AST 4) noch das Abmahnschreiben vom 26.03.2021 (Anlage AST 6) wurden der Antragsgegnerin ordnungsgemäß zugestellt.

2.7.1 Kein Zugang des Hinweisschreibens vom 23.03.2021

Das Hinweisschreiben des Verfahrensbevollmächtigten der Antragstellerin vom 23.03.2021 ist der Antragsgegnerin nicht ordnungsgemäß zugegangen.

Es wird bestritten, dass die Antragstellerin das Hinweisschreiben vom 23.03.2021 postalisch an die Antragsgegnerin versandt hat. Der Antragsgegnerin ist ein derartiges Schreiben nicht per Post zugegangen.

Glaubhaftmachung: 1. Eidesstattliche Versicherung [redacted], als **Anlage AG 6**.

2. Eidesstattliche Versicherung [redacted], als **Anlage AG 7**.

Auch via E-Mail ist der Antragsgegnerin das Hinweisschreiben vom 23.03.2021 nicht ordnungsgemäß zugestellt worden.

Nach der Zustellung der Beschlussverfügung rekonstruierte die Antragsgegnerin, dass die Antragstellerin die E-Mail-Adresse support@quad9.net verwendete. Dies ist eine E-Mail-Adresse, die für technische Anfragen zum Dienst der Antragsgegnerin eingerichtet ist. Alle an diese E-Mail-Adresse gerichteten Nachrichten werden automatisiert an das Ticket-System des Herstellers Zendesk der Antragsgegnerin geschickt. Das Produkt Zendesk verfügt über eigene Spamfilter und diesbezügliche Richtlinien, die von den Nutzern nicht abgeschaltet werden können. Zendesk erstellt aus den eingehenden, nicht als Spam erkannten, E-Mails automatisiert Tickets zur weiteren Bearbeitung durch Supportpersonal. Ein solches Ticket wurde lediglich für eine E-Mail vom 26.03.2021 erstellt.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

Dies legt den Verdacht nahe, dass weitere E-Mails von Zendesk als Spam eingestuft und nicht zur Kenntnis des Supportpersonals gebracht wurden. Eine Kenntnisnahme des Inhaltes des Hinweisschreibens der Antragstellerin vom 23.03.2021 erfolgte für die Antragsgegnerin mithin erst durch die Zustellung der Beschlussverfügung.

Die Antragsgegnerin betreibt für Fälle mit rechtlichen Implikationen unter abuse@quad9.net eine dem Industriestandard entsprechende E-Mail-Adresse (RFC2142), die speziell für Abuse-Meldungen, also auch für Hinweise auf rechtswidriges Verhalten, eingerichtet ist.

Glaubhaftmachung: 1. Screenshots von Websites https://www.peeringdb.com/net/17212, Whois-RWS, ipinfo und ipasn, als **Anlage AG 8,**

2. Eidesstattliche Versicherung [redacted], als **Anlage AG 3.**

Unter den angegebenen Quellen sind die Kontaktmöglichkeiten veröffentlicht, so für die Antragsgegnerin auch der Abusekontakt. Dies hätte die Antragstellerin wissen müssen. In diesem für Abuse-Fälle vorgesehenen E-Mail-Postfach gibt es keine nennenswerte Spam-Filterung, so dass die Kenntnisnahme der Mail über diesen Kanal als sicher vorauszusetzen

ist. Die Antragsgegnerin nimmt Abuse-Meldungen ernst und über diesen Kanal eingehende Nachrichten werden direkt an das Management weitergeleitet und dort bearbeitet.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

2.7.2 Kein Zugang des Abmahnschreibens vom 26.03.2021

2.7.2.1 Kein Zugang vorab per E-Mail

Die Antragstellerin führt an, dass sie die Antragsgegnerin mit Schreiben vom 26.03.2021 abmahnte. Sie behauptet, dass ein Gutachten über die urheberrechtsverletzenden Inhalte auf der beanstandeten Domain dem Schreiben beigefügt worden sei. Ausweislich der Anlage AST 6 wurde dem Schreiben kein Gutachten beigefügt, da dieses nicht in der Anlage enthalten ist. Das Schreiben enthält auch keinen Anlagenvermerk.

Das Abmahnschreiben wurde der Antragsgegnerin ebenfalls nicht wirksam zugestellt. Die Antragsgegnerin stellte erst nach der Zustellung der Beschlussverfügung fest, dass die E-Mail vom 26.03.2021 im Support-Postfach der Antragsgegnerin einging und ein Ticket erstellt wurde. Dieses wurde nicht weiter bearbeitet. Die Antragsgegnerin vermutet, dass es von den Support-Mitarbeitern, die nicht mehr bei Quad9 beschäftigt sind, ignoriert wurde, da die Mail für einen Phishing-Versuch gehalten wurde. Es ist Teil der Schulung für Support-Mitarbeiter, keine Anhänge zu öffnen, es sei denn, es gibt Anhaltspunkte, dass der Nutzer einen Anhang erkennbar in gutem Glauben sendet. Da der Service der Antragsgegnerin kostenlos ist, gibt es keine Verpflichtung zur Antwort an Anfragende, so dass ein unbeantwortetes Ticket nicht automatisch auffällt.

Die E-Mail des Verfahrensbevollmächtigten der Antragstellerin enthielt neben einer Fußzeile nur den Text „Zur sofortigen Kenntnisnahme, Achtung Fristsache!“ sowie einen Anhang im pdf-Format.

Glaubhaftmachung:

1. Kopie E-Mail v. 26.03.2021, als **Anlage AG 9.**

2. Eidesstattliche Versicherung [redacted] und Übersetzung aus der englischen in die deutsche Sprache, als **Anlage AG 4**.

Bei E-Mails aus unbekannten Quellen hält auch der Vorstand des eco Verband der Internetwirtschaft e.V. und Berater für Cybersicherheit [redacted] in seiner Eidesstattlichen Versicherung fest, dass aus Sicherheitsgründen dringend dazu geraten werden muss, Anlagen zu E-Mails aus unbekannter Quelle nicht zu öffnen um einer Infektion des eigenen Rechners mit Malware vorzubeugen.

„Die Sicherheitsrichtlinie von Unternehmen sollte als grundsätzlichen Sicherheitsaspekt beim Empfang von Emails vorsehen, keine Anhänge unbekannter Absender zu öffnen. Dieses Vorgehen ist Bestandteil jeder erfolgreichen Sicherheitszertifizierung (IT-Grundschutz, ISO

27001) und entspricht den allgemeinen Empfehlungen der Experten, so z.B. des Bundesamts für Sicherheit in der Informationstechnik oder Heise Security:

> „Das BSI rät daher dringend davon ab, den Anhang von E-Mails unbekannter Absender zu öffnen." (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Infizierte-Systeme-bereinigen/infizierte-systeme-bereinigen_node.html.)
>
> „Der wichtigste Grundsatz für den sicheren Umgang mit E-Mails lautet daher, niemals einen Dateianhang zu öffnen, den man nicht angefordert hat." (Heise Security, https://www.heise.de/security/dienste/Dateianhaenge-472901.html)

Ausnahmen hiervon sollten nur dann gemacht werden, wenn der Absender eindeutig identifiziert und verifiziert werden kann, z.B. durch die Verwendung signierter Emails.

Für eine Kontaktaufnahme über zentrale Adressen (noc, abuse, hostmaster) sollten alle relevanten Informationen im Textteil der E-Mail enthalten sein. Bei Dateianhängen sollte auf Binärdateien (.exe., .zip, .pdf) verzichtet werden, um eine Bearbeitung beim Empfänger zu gewährleisten."

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

2.7.2.2 Kein Zugang per Post an den Zustellungsbevollmächtigten

Das von der Antragstellerin versandte Abmahnschreiben vom 26.03.2021 ist der Zustellungsbevollmächtigten der Antragsgegnerin, nicht per Post zugegangen. Der Zugang des Schreibens wird bestritten.

Glaubhaftmachung:

1. Eidesstattliche Versicherung [redacted], als **Anlage AG 6**.

2. Eidesstattliche Versicherung [redacted], als **Anlage AG 7**.

Die Zustellungsbevollmächtigte für die Antragsgegnerin für sämtliche Korrespondenz, die bei der Schweizer Adresse Werdstrasse 2 in 8004 Zürich, eingeht, ist die Schweizer Stiftung SWITCH. Sie ist die Betreiberin des Schweizer Wissenschaftsnetzes der Hochschulen. Für die Verwaltung des Posteingangs der Antragsgegnerin sind [redacted] und [redacted] verantwortlich. Beide haben eidesstattlich versichert, dass kein Posteingang von dem Verfahrensbevollmächtigten der Antragstellerin für die Antragsgegnerin zu verzeichnen war. Lediglich die Beschlussverfügung des LG Hamburg mit dem Aktenzeichen 310 O 99/21 wurde an die Werdstrasse 2 in 8004 Zürich zugestellt und auch unverzüglich an die Antragsgegnerin weitergeleitet.

Glaubhaftmachung: 1. Eidesstattliche Versicherung [redacted], als **Anlage AG 6**.

2. Eidesstattliche Versicherung [redacted], als **Anlage AG 7**.

2.7.2.3 Kein Zugang des Schreibens vom 08.04.2021

Auch das weitere Abmahnschreiben des Verfahrensbevollmächtigten der Antragstellerin vom 08.04.2021 ist der Antragsgegnerin nicht übermittelt worden. Da die E-Mail des Verfahrensbevollmächtigten der Antragstellerin vom 26.03.2021 nicht direkt im Spam-Ordner landete, wurde automatisch ein Ticket erzeugt. Dadurch wurde eine Ticketnummer generiert (15321) und eine automatische Nachricht an den Verfahrensbevollmächtigten der Antragstellerin geschickt, dass die E-Mail eingegangen ist und weitere Kommunikation in der Sache als Antwort auf diese automatisch generierte E-Mail geschickt werden soll. Auf diese automatisch versendete Antwort hin antwortete der Verfahrensbevollmächtigte der Antragstellerin nicht, sondern versandte eine neue E-Mail, die denselben Text wie die E-Mail vom 26.03.2021 enthielt. Ein Ticket wurde dazu vom System nicht erstellt, sodass davon auszugehen ist, dass auch diese E-Mail durch den Spamfilter aussortiert wurde.

2.7.3 Keine hinreichende Inanspruchnahme anderer Beteiligter

Die Antragstellerin behauptet, sie habe umfangreiche Anstrengungen unternommen, um das rechtsverletzende Angebot unter Einschaltung von vorrangig in Anspruch zu nehmenden Beteiligten abzustellen. Die Antragstellerin behauptet, dass sie die Daten des Betreibers der Website [redacted] wegen eines fehlenden Impressums nicht ermitteln kann. Das Vorhalten eines Impressums ist nicht nach jeder Rechtsordnung erforderlich, so dass die Anstrengungen der Antragstellerin keinesfalls mit der Suche nach einem Impressum enden dürfen.

Wie bereits dargelegt, sind die Schreiben der Antragsgegnerin nicht zugegangen. Mithin muss davon ausgegangen werden, dass auch anderen etwaigen Beteiligten keine Hinweisschreiben zugegangen sind. Es wird bestritten, dass den anderen Beteiligten die Hinweisschreiben zugingen.

Fraglich ist, welche Bemühungen die Antragstellerin überhaupt unternahm, um den konkreten Rechtsverstoß, die Abrufbarkeit des Musikalbums [redacted], durch andere Beteiligte beseitigen zu lassen.

Die verfahrensrelevanten Hinweisschreiben des Verfahrensbevollmächtigten der Antragstellerin wurden angeblich am 23.03.2021 erstellt. Bereits drei Tage später, mit Schreiben vom 26.03.2021, nahm die Antragstellerin die Antragsgegnerin bereits mittels kostenpflichtiger Abmahnung als Störerin in Anspruch. Ausweislich des Abmahnschreibens (Anlage AST 6) forderte die Antragstellerin die Betreiber der beanstandeten Domain erstmals am 23.03.2021 zur Löschung rechtsverletzender Inhalte auf. Die Inanspruchnahme der Antragsgegnerin und der Täter der geltend gemachten Rechtsverletzung erfolgte somit zeitgleich. In diesem Zusammenhang wird vorsorglich die zwischen Hinweis und Abmahnung liegende viel zu kurze Fristsetzung gerügt.

Das Vorgehen der Antragstellerin legt nahe, dass ihr primäres Ziel die kostenpflichtige Inanspruchnahme der Antragsgegnerin ist. Zumindest muss unterstellt werden, dass etwaige Hinweisschreiben an die anderen Beteiligten lediglich pro forma, nicht aber in dem ernsthaften Bestreben ergangen sind, Abhilfe zu schaffen oder den vermeintlich Angeschriebenen hinreichend Gelegenheit zur Abhilfe zu geben.

2.7.3.1 Keine Inanspruchnahme der Registry

Eine Inanspruchnahme der kommerziell betriebenen Registry der Domain [redacted] durch die Antragstellerin erfolgte nicht. Domains mit der Endung „.to", der Länderendung für Tonga, werden von der Tonic Domain Corporation mit Sitz in den USA verwaltet. Laut deren Webseite ist die Registry unter folgender Anschrift zu erreichen: Tonic Domains Corp., P.O. Box 42, Pt San Quentin, CA 94964, U.S.A.

Glaubhaftmachung: Screenshot von der Website der Registrierungsstelle Tonic unter https://www.tonic.to/faq.htm, als **Anlage AG 10.**

Die Registry Tonic schreibt auf Ihrer Website:

"...any activities deemed by Tonic to be inappropriate or illegal may be removed from the .TO zonefile without notice to the registrant."

Die Registry behält sich damit das Recht vor, das Auflösen einer rechtsverletzenden Domain zu unterbinden.

Glaubhaftmachung: Screenshot von der Website der Registrierungsstelle Tonic unter https://www.tonic.to/faq.htm, als **Anlage AG 10**.

Tonic unterhält eine vertragliche Beziehung zu dem Domaininhaber von [redacted] und kann insofern auch vertragliche Sanktionen „an der Quelle" umsetzen und damit die Funktionalität der Domain global unterbinden.

Für eine Kontaktaufnahme mit der Registry Tonic, damit diese die Domain sperrt, ist nichts dargetan. Damit erschöpfen sich die Möglichkeiten gegenüber Tonic jedoch nicht, mit dem Domaininhaber in Kontakt zu treten.

In den „FAQs", den häufig gestellten Fragen und den Antworten der Registry, heißt es zudem:

> *„When you attempt to register a name that is already registered, the web page that is returned has a link that sends your contact email address to the registrant. Whether they choose to reply to your email or not is up to them."*

Glaubhaftmachung: Screenshot von der Website der Registrierungsstelle Tonic unter https://www.tonic.to/faq.htm, als **Anlage AG 10**.

Wenn der Versuch unternommen wird, eine bereits registrierte Domain zu registrieren, wird auf Wunsch die E-Mail-Adresse an den Domaininhaber mit der Bitte um Kontaktaufnahme

übermittelt, über die der Domaininhaber angeschrieben werden kann. Dafür, dass die Antragstellerin von dieser Möglichkeit Gebrauch gemacht hat, ist ebenfalls nichts dargetan.

Auch der Hinweis darauf, dass keine Whois-Daten zu ermitteln seien, ist nicht hinreichend. Die Antragstellerin hat nichts dafür dargetan, bei der Registry eine Auskunft über die Daten des Domaininhabers angefragt zu haben.

Mit Inkrafttreten der DSGVO haben weltweit eine Vielzahl von Registries ihre Praxis geändert und keine personenbezogenen Daten mehr im öffentlichen Whois veröffentlicht. Rechteinhaber sowie andere Interessenten an nicht veröffentlichten Registrierungsdaten sind insofern auf Anfragen bei den Registries oder Registraren verwiesen.

Glaubhaftmachung: Eidesstattliche Versicherung [redacted], als **Anlage AG 3**.

2.7.3.2 Keine Inanspruchnahme des Registrars

Ein Registrar ist eine Organisation beziehungsweise ein Unternehmen, das Registrierungen von Domains durchführt. Viele Registries ermöglichen nicht direkt, sondern nur über Registrare die Registrierung von Domains. Die Antragstellerin hat nichts dazu dargetan, ob im vorliegenden Fall die Domain über einen Registrar registriert wurde und ob ein Registrar kontaktiert wurde, um gegebenenfalls das Auflösen der Domain zu unterbinden oder die Domain zur Löschung zu bringen.

2.7.3.3 Keine hinreichende Geltendmachung eines Auskunftsanspruchs gegenüber dem Zahlungsdienstleister

Die Betreiber der beanstandeten Domain nehmen Zahlungen über den Anbieter [redacted] entgegen. Dieser muss denknotwendig entweder die Identität oder zumindest eine Information dazu von den Betreibern der beanstandeten Domain verfügen, um Gelder weiterleiten zu können, die hätte angefragt werden können. Der Sachvortrag der Antragstellerin lässt nicht erkennen, dass hinreichend deutlich und substantiiert an den Zahlungsdienstleister herangetreten wurde. Zudem ist der Zugang des Schreibens nicht dargetan.

2.7.4 Kein hinreichender Sachvortrag zur Rechtswidrigkeit des Angebots

Die Empfehlung des Prüfungsausschusses Clearingstelle Urheberrecht im Internet (CUII) vom 09.03.2021 zur Umsetzung einer DNS-Sperrung bzgl. [redacted] ist der Antragsgegnerin ebenfalls erst mit der Übermittlung der Antragsschrift durch den Verfahrensbevollmächtigten der Antragstellerin, mithin nach Erlass der Beschlussverfügung zur Kenntnis gelangt.

Die Ausführung des Prüfungsausschusses, dass eine klare Rechtsverletzung durch die Bereithaltung von Links durch die Betreiber von [redacted] vorliegt, wird bestritten.

Um Informationen auf der Plattform [redacted] hochladen zu können, ist es erforderlich, dass der Nutzer ein Konto – mit einem Benutzernamen und einem Passwort – einrichtet und eine E-Mail-Adresse angibt. Ein von einem Nutzer hochgeladener Downloadlink wird dann online gestellt. Ausweislich der Registrierungsbedingungen der Plattform [redacted] ist es den Nutzern jedoch untersagt, Urheberrechtsverstöße über die Plattform zu begehen.

Glaubhaftmachung: Screenshot von den Nutzungsbedingungen der Website [redacted] unter [redacted], als **Anlage AG 11**.

Diese Ausführungen lassen darauf schließen, dass Urheberrechtsverstöße seitens der Betreiber der Plattform [redacted] nicht geduldet werden. Nicht erklärlich ist, warum die Antragstellerin das Gutachten der CUII nicht im Zuge der ersten Kontaktaufnahme mitschickte, um eine Nachvollziehbarkeit der behaupteten Rechtsverletzung und deren zügige Beseitigung zu ermöglichen.

2.7.5 Erstmalige Kenntnisnahme durch Verfügungsbeschluss vom 12.05.2021

Nach alldem steht fest, dass die Antragsgegnerin erstmalig mit Zustellung des Beschlusses des Landgerichts Hamburg am 12.05.2021 auf den Vorgang insgesamt hingewiesen wurde. Im Anschluss hat die Antragsgegnerin den Vorgang sodann in rechtlicher und tatsächlicher Hinsicht prüfen lassen und im Anschluss in zeitlich angemessener Frist die ihr zur Verfügung stehenden technischen Maßnahmen ergriffen, um die angeblich in die Rechte der Antragstellerin eingreifenden Inhalte einzuschränken. Mithin handelte die Antragsgegnerin fristwahrend und kann nicht im Wege des Verfügungsverfahrens als Störerin in Anspruch genommen werden, da die Antragstellerin weder das Hinweisschreiben vom 23.03.2021 noch die angeblich nachfolgenden Abmahnschreiben, der Antragsgegnerin zustellte. Dieses Versäumnis geht zu Lasten der Antragstellerin.

3. Eingang des Antrags auf Erlass einer einstweiligen Verfügung

Die Antragstellerin macht durch die eidesstattliche Versicherung [redacted] (Anlage AST 3) glaubhaft, dass sie Kenntnis von der Rechtsverletzung am 11.03.2021 erlangte. Der Antrag auf Erlass einer einstweiligen Verfügung ist am 12.04.2021 bei Gericht eingegangen

II. Rechtliche Würdigung

A. Unzulässigkeit

Der Antrag auf Erlass einer einstweiligen Verfügung ist unzulässig.

1. LG Hamburg örtlich unzuständig

Das Landgericht Hamburg ist nicht örtlich zuständig gemäß § 32 ZPO.

Die Zuständigkeit des Gerichts in einstweiligen Verfügungsverfahren folgt aus der Zuständigkeit für eine - hypothetische - Hauptsache gemäß § 937 Abs. 1 i. V. m. § 943 Abs. 1 Alt. 1 ZPO (vgl. Vollkommer, in: Zöller, ZPO, 32. Aufl. 2018, § 919 Rn. 9).

Der Erfolgsort einer unerlaubten Handlung im Sinne von § 32 ZPO besteht bei einer behaupteten Verletzung des Urheberrechts oder verwandter Schutzrechte durch ein öffentliches Zugänglichmachen des Schutzgegenstands über eine Internetseite im Inland, wenn die geltend gemachten Rechte im Inland geschützt sind und die Internetseite im Inland öffentlich zugänglich ist (vgl. BGH, Urteil v. 21.04.2016 - I ZR 43/14 - An Evening with Marlene Dietrich, juris Rn. 18). Zur Begründung der Zuständigkeit reicht die schlüssige Behauptung von Tatsachen aus, auf deren Grundlage sich eine im Gerichtsbezirk begangene unerlaubte Handlung ergibt. Die Vorschriften über die örtliche Zuständigkeit (§§ 12 ff. ZPO) regeln mittelbar auch die Grenzziehung zwischen der Zuständigkeit deutscher und ausländischer Gerichte (vgl. BGH, Urteil v. 02.03.2010 - VI ZR 23/09, juris Rn. 7 m.w.N.).

Die Antragstellerin stützt ihre Ansprüche darauf, dass das streitgegenständliche Musikalbum über die im Tenor aufgeführte Internetseite unter den in der Antragsschrift angegebenen URLs ohne Zustimmung der Antragstellerin öffentlich zugänglich gemacht worden sei und diese in Deutschland abrufbar waren. Eine Rechtsverletzung auf dem Gebiet der Bundesrepublik Deutschland begründet nach zutreffender Auffassung des AG Hamburg jedoch keine Allzuständigkeit sämtlicher Gerichte in der Bundesrepublik Deutschland:

> *„Auch wenn es im presserechtlichen Kontext einen Senat des BGH geben mag, der die These von der Allzuständigkeit sämtlicher Gerichte der Republik in Fällen der hier vorliegenden Art teilt, so wird doch aus anderer Rechtsprechung des BGH hinreichend deutlich, dass es auch BGH-Senate gibt, die den teleologischen Erwägungen und den Folgerungen aus dem verfassungsrechtlichen Gebot des gesetzlichen Richters maßgebliche Bedeutung beimessen. Eine gefestigte Rechtsprechung erscheint insoweit noch nicht gegeben. Auch eine einschlägige Entscheidung des BVerfG ist noch nicht ersichtlich. So hat der BGH für die vergleichbare Problematik bei der Begründung internationaler Zuständigkeit deutscher Gerichte im Rahmen von Urheberrechtsverletzungen angemerkt, dass „viel für die Begrenzung einer ansonsten bestehenden Vielzahl von Gerichtsständen auf diejenigen, in deren Zuständigkeitsbereich eine Interessenkollision tatsächlich eingetreten sein kann spreche“ (AG Hamburg, Urteil v. 30.01.2014 – 22a C 100/13).*

Da die Antragsgegnerin keinen Geschäftssitz innerhalb der Bundesrepublik Deutschland vorhält, wäre eine Einreichung des Antrags auf einstweiligen Rechtschutz am Geschäftssitz der Antragstellerin eine relevante Gerichtsstandbegründung.

Ein Bezug zum Gerichtsstandort Hamburg besteht unter keinem Gesichtspunkt. Die Gerichtsstandortwahl der Antragstellerin ist rechtsmissbräuchlich. Ein rechtsmissbräuchliches Vorgehen wird angenommen, wenn eine gezielte Auswahl des Gerichtsstands, die auf eine

Benachteiligung der Antragsgegnerin abzielt, erkennbar ist (vgl. OLG Brandenburg, Urteil v. 28.11.2016 - 1 U 6/16, juris, Rn. 34).

Das OLG München entschied, dass ein Verfügungsgrund ausscheidet, wenn der Antragsteller mehr als einen Monat mit dem Antrag auf Erlass einer einstweiligen Verfügung nach Kenntnisnahme eines Rechtsverstoßes zuwartet:

> *„Ein Verlag, der Kenntnis davon hat, dass auf einem Internetportal vorwiegend urheberrechtlich geschützte Werke, u.a. Werke, an denen er die Rechte innehat, illegal öffentlich zugänglich gemacht werden, und einem Vorgehen gegen den Portalbetreiber und/oder seinen Hostprovider jede Erfolgsaussicht fehlt, verhält sich dringlichkeitsschädlich, wenn er gegen den Access-Provider nicht innerhalb eines Monats ab Erlangung dieser Kenntnis den Erlass einer einstweiligen Verfügung beantragt. Die Dringlichkeitsfrist beginnt nicht mit der Kenntnis der Verletzung der Rechte hinsichtlich jedes neu öffentlich zugänglich gemachten Werks neu zu laufen."*
>
> *Der Annahme der Dringlichkeit kann ein Verhalten des Antragstellers entgegenstehen, dem zu entnehmen ist, dass er die Angelegenheit selbst nicht als dringend ansieht. Nach ständiger Rechtsprechung der für die Gebiete des gewerblichen Rechtsschutzes und des Urheberrechts zuständigen Senate des Oberlandesgerichts München kann nicht mehr von Dringlichkeit ausgegangen werden, wenn ein Antragsteller länger als einen Monat ab Erlangung der Kenntnis von der Verletzungshandlung und der Person des Verletzers zuwartet, bevor er den Erlass einer einstweiligen Verfügung beantragt (OLG München, Urteil v. 02.02.2019 – 29 U 3889/18).*

Die Monatsfrist lief – auch unter Berücksichtigung des offiziellen Release – ab, weshalb zum Zeitpunkt der Antragstellung keine Dringlichkeit mehr vorlag.

Aufgrund des Geschäftssitzes der Antragstellerin wäre der Gerichtsstand München begründet. Das örtlich zuständige LG München hätte entsprechend der Auffassung des OLG München den Verfügungsgrund verneint. Demnach wurde der örtliche Gerichtsstandort Hamburg mit gezielter Benachteiligungsabsicht gegenüber der Antragsgegnerin von der Antragstellerin gewählt.

2. Unzulässiger Antrag

2.1 Unbestimmter Antrag

Der Antrag ist nicht hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO.

Nach § 253 Abs. 2 Nr. 2 ZPO darf ein Verbotsantrag nicht derart unbestimmt gefasst sein, dass Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts (§ 308 Abs. 1 S. 1 ZPO) nicht erkennbar abgegrenzt sind, sich die Antragsgegnerin deshalb nicht erschöpfend verteidigen kann und letztlich die Entscheidung darüber, was der Antragsgegnerin verboten ist, dem Vollstreckungsgericht überlassen bleibt. Der Gebrauch von allgemeinen Begriffen im Verfügungsantrag zur Bezeichnung der zu untersagenden Handlung „öffentliche Zugänglichmachung" genügt nicht, wenn der der Antragsgegnerin vorgeworfene Beitrag nicht

ersichtlich ist. Der Antragsgegnerin wird in der Begründung eine Unterstützungshandlung zur öffentlichen Zugänglichmachung vorgeworfen. Im Antrag wird die Antragsgegnerin jedoch als Täterin in Anspruch genommen. Der Verfügungsantrag bezieht sich mithin nicht auf eine Störerhaftung, er enthält eine Tathandlung der Antragsgegnerin durch die Bereitstellung von Hyperlinks. Die Parteien dürften sich einig sein, dass die Antragsgegnerin keine Hyperlinks setzt. Der Umstand, dass die Antragstellerin auf Seite 12 der Antragsschrift eine Störerhaftung annimmt, relativiert nicht eine falsche Antragsfassung. Im Gegenteil kann diese nicht zur Auslegung herangezogen werden, da die Antragsbegründung dem Antrag widerspricht. Auch die Kammer vertritt die Ausfassung, dass der Antrag nicht hinreichend das zu unterlassende Verhalten darlegt, da die erfolgte „Antragskorrektur" durch die Kammer aufzeigt, dass der Antrag der Antragstellerin unbestimmt ist. Auch die nach dem Hinweis der Kammer erfolgte „Präzisierung" des Antrages durch die Antragstellerin ist nicht hinreichend bestimmt.

2.2 Unzulässige Antragsänderung

Ferner ist die „Antragskorrektur" der Kammer als eine Antragsänderung zu werten, die den Rahmen einer zulässigen Antragskorrektur überspannt. Die durch die Kammer vorgenommene Konkretisierung im Antrag, welche die tatsächliche Handlung beschreibt, lässt erst erkennen, welche zu unterlassene Handlung von der Antragsgegnerin verlangt wird.

B. Unbegründetheit

Der Antrag auf Erlass einer einstweiligen Verfügung ist unbegründet.

1. Kein Verfügungsanspruch

Der Antragstellerin steht gegenüber der Antragsgegnerin kein Anspruch zu.

1.1 Keine Aktivlegitimation der Antragstellerin

Die Antragstellerin ist nicht aktivlegitimiert.

Bei der Verletzung urheberrechtlicher Nutzungs- und Verwertungsrechte ist zunächst der Urheber bzw. der Inhaber des verwandten Schutzrechts allein aktivlegitimiert. Nach § 2 Abs.1, 7 UrhG steht der Urheberschutz originär demjenigen zu, der das Werk persönlich herstellt. Zur Geltendmachung von Ansprüchen nach den §§ 97 ff. UrhG ist auch der Inhaber eines ausschließlichen Nutzungsrechts an dem jeweiligen Werk berechtigt. Sind Rechte einem anderen als Nutzungsberechtigten eingeräumt worden, kommt es für die Aktivlegitimation darauf an, in welchem Umfang diese Rechte übertragen worden sind. Dabei reicht die Aktivlegitimation so weit, wie die räumlichen, sachlichen und zeitlichen ausschließlichen Nutzungsrechte reichen (Dreier/Schulze/Specht UrhG 5. Aufl., § 97 Rn. 19).

Der Vortrag der Antragstellerin, dass eine Ablichtung des Back-Covers der CD [redacted], auf dem die Antragstellerin durch den P-Vermerk als exklusive Inhaberin der Tonträgerherstellerrechte ausgewiesen sei, reicht für die die Vermutung nach §§ 85 Abs.

4, 10 Abs. 1 UrhG nicht aus. Grund ist, dass auch nach den Vorschriften des Art. 11 des Rom-Abkommens über die Anbringung des P-Vermerks nicht sichergestellt sei, dass das in dem P-Vermerk genannte Unternehmen tatsächlich Inhaber des Tonträgerherstellerrechts sei.

1.2 Haftungsprivilegierung nach §§ 8 Abs. 1, 9 TMG

Entgegen der Ansicht der Kammer kann sich die Antragsgegnerin auf eine Haftungsprivilegierung für Diensteanbieter gem. §§ 8 Abs. 1, 9 TMG, jedenfalls in analoger Anwendung, berufen. Eine Haftung der Antragsgegnerin auf Unterlassung ist nach §§ 8 Abs. 1 S. 2, 9 i.V.m. § 8 Abs. 1 S. 2 TMG ausgeschlossen.

1.2.1 Anwendbarkeit des TMG

Die Haftungsausschlüsse gem. §§ 7 ff. TMG sind vorliegend anwendbar. Die Antragsgegnerin ist Diensteanbieterin i.S.v. § 2 Nr. 1 TMG. Diensteanbieter ist danach jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Der Begriff des Diensteanbieters im TMG geht auf die E-Commerce-Richtlinie (RL 2000/31/EG) zurück und ist als autonomer Begriff des Unionsrechts einheitlich auszulegen. In Art. 2 lit. b der E-Commerce-Richtlinie wird „Diensteanbieter" als jede natürliche oder juristische Person, die einen Dienst der Informationsgesellschaft anbietet, definiert. Der Begriff „Dienst der Informationsgesellschaft" ist ein ebenfalls ein autonomer Begriff des Unionsrechts, der in Art. 1 Abs. 1 lit. b der RL (EU) 2015/1535 als „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung" legaldefiniert ist. Dies trifft auf die Dienstleistung der Antragsgegnerin zu. Die Antragsgegnerin erbringt auf individuellen Abruf ihrer Nutzer eine Dienstleistung, die in der Auflösung der Domain in eine numerische IP-Adresse und deren Übermittlung besteht. Dass die Antragsgegnerin diese Dienstleistung unentgeltlich erbringt, ist unschädlich. Denn zum einen kommt es für die Entgeltlichkeit nicht darauf an, dass die jeweiligen Nutzer das Entgelt entrichten. Es genügt, wenn die Dienstleistung anderweitig finanziert wird, etwa durch Werbung oder wie vorliegend durch Spenden (EuGH, Urt. vom 15. September 2016, Rs. C-484/14 – *McFadden,* Rn. 41, 43). Zum anderen stellt die Legaldefinition der RL (EU) 2015/1535 darauf, ab, dass die Dienste „in der Regel" entgeltlich erbracht werden. Dies trifft auf den Betrieb eines DNS-Resolvers zu, dessen Betrieb regelmäßig entgeltlich ist. Wie oben dargelegt, nutzt eine große Anzahl der Internetnutzer den voreingestellten DNS-Resolver ihres Internet-Service-Providers, der diese Leistung als Teil seiner vertraglich geschuldeten Leistung und durch entsprechende Vertragstarife abgegoltenen Geschäftsmodells anbietet.

Die RL (EU) 2015/1535 führt in Anhang 1 ferner eine Beispielliste von Diensten auf, die dieser Definition *nicht* unterfallen. DNS-Dienste werden in Anhang 1 nicht genannt.

Dieses Ergebnis deckt sich mit der Rechtsprechung des BGH zur Auslegung des Diensteanbieter-Begriffs im TMG. Nach der Rechtsprechung des BGH ist der Begriff des Diensteanbieter funktionell auszulegen. Der Diensteanbieter muss durch seine Weisungen oder Herrschaftsmacht über Rechner und Kommunikationskanäle die Verbreitung oder das Speichern von Informationen ermöglichen und nach Außen als Erbringer von Diensten

auftreten (BGH, Urt. vom 15.10.2020 – I ZR 13/19, Rn. 16 mit Verweis auf Spindler in Spindler/Schmitz, TMG, 2. Aufl. § 2 Rn. 28). Dies trifft auf die Antragsgegnerin zu. Die Antragsgegnerin betreibt Rechner in ihrer Herrschaftsmacht und verbreitet durch die Weitergabe von DNS-Anfragen Informationen. Für ihre Nutzer, die den Dienst der Antragsgegnerin in Anspruch nehmen, tritt diese als Erbringer von Diensten nach Außen auf.

Anders als der Registrar, den der BGH nicht als Diensteanbieter i.S.v. § 2 Nr.1 TMG einstuft, weil er lediglich die administrative Abwicklung der Domainregistrierung vornehme, knüpft die Störerhaftung der Antragsgegnerin vorliegend an einen Beitrag an, der jeweils bei der Vermittlung des Abrufs der beanstandeten Domain erbracht wird (BGH, Urt. vom 15.10.2020 – I ZR 13/19, Rn. 16). Die Antragsgegnerin ist, anders als der Registrar, mithin selbst an der technischen Zugangsvermittlung beteiligt (BGH, Urt. vom 15.10.2020 – I ZR 13/19, Rn. 17). Die automatisierte Auflösung von Domainnamen in IP-Adressen ist für jeden Abruf der Domain erforderlich. Der Registrar ist nach der einmaligen Konnektierung der Domain an späteren Abrufen nicht mehr beteiligt.

1.2.2 Antragsgegnerin ist nach § 8 Abs. 1 TMG haftungsprivilegiert

Die Antragstellerin kann sich auf die Haftungsprivilegierung gem. § 8 Abs. 1 S. 1 TMG berufen. Nach § 8 Abs. 1 S. 1 TMG sind Diensteanbieter für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang vermitteln, unter den nachfolgend in Ziffern 1 – 3 genannten Voraussetzungen nicht verantwortlich und können nach § 8 Abs. 1 S. 2 TMG weder auf Schadensersatz, noch auf Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden.

Der Dienst der Antragsgegnerin erfüllt die Voraussetzungen aus § 8 Abs. 1 S. 1 2. Alt TMG, da sie ihren Nutzern Zugang zu fremden Informationen vermittelt. Die Antragsgegnerin erbringt als unabhängiger DNS-Resolver eine Dienstleistung, die ihren Nutzern den Zugang zu den unter den jeweils abgefragten Domains vorgehaltenen Diensten vermittelt. Erst indem der Dienst der Antragsgegnerin durch die Abfrage der IP-Adressen dem Browser der Nutzer die so ermittelten Antworten übermittelt, erhalten die Nutzer Zugang zu den jeweiligen Websites.

Auch bei der Beurteilung, ob die Haftungsprivilegierung nach § 8 Abs. 1 S. 1 2. Alt. TMG einschlägig ist, muss auf den konkreten Abrufweg abgestellt werden. Das erkennende Gericht stellt bei seiner rechtlichen Würdigung des Beitrags der Antragsgegnerin auf die Abrufbarkeit rechtswidriger Angebote über den spezifischen Abrufweg unter der Nutzung des DNS-Resolvers der Antragsgegnerin ab. Für diesen Abrufweg stellt die Auflösung der Domainnamen in IP-Adressen eine Zugangsvermittlung dar. Denn bei Beibehaltung der konkreten DNS-Einstellungen und Nutzung des DNS-Resolvers der Antragsgegnerin wäre die Auffindbarkeit und der Zugang zu den jeweiligen Websites unter den im Browser eingegebenen Domainnamen nicht möglich.

Dem entsprechen auch die Feststellungen des erkennenden Gerichts, das das Geschäftsmodell der Antragsgegnerin als „Vermittlung des Zugangs zum Internet“ beschreibt. Das Gericht stellt zutreffend fest, dass die auf der Website [redacted]

veröffentlichten Informationen für die Nutzer der Antragsgegnerin erst mittels der durch die Antragsgegnerin erbrachte Übersetzung von IP-Adresse in Domainnamen zugänglich würden. Ohne die Auflösung des Domainnamens in die IP-Adresse ist, wie das erkennende Gericht weiter feststellt, den Nutzern der Antragsgegnerin der Zugriff zu Websites verwehrt. Die Dienstleistung der Antragsgegnerin besteht auch nach diesen Feststellungen in der Vermittlung des Zugangs zu Informationen. Es ist nicht dargetan oder ersichtlich, dass der Begriff der Vermittlung des Zugangs i.S.v. § 8 Abs. 1 S. 1 2. Alt. TMG in dem Sinne eng verstanden werden müsse, dass er nur die unmittelbare Eröffnung des Zugangs zu bestimmten Informationen erfasse. Der Begriff „Vermittlung" drückt sprachlich bereits aus, dass auch solche Beiträge, die den Zugang nicht unmittelbar eröffnen, sondern durch Vermittlung ermöglichen, privilegiert sein sollen. Wird wie vorliegend eine Kette von Diensteanbietern für die Vermittlung des Zugangs zu einer Information genutzt, bei der jeder Diensteanbieter automatisch den Zugang zum nächsten Diensteanbieter vermittelt, sind sämtliche Diensteanbieter in dieser Kette gem. § 8 TMG privilegiert (MüKo StGB, 3. Aufl. 2019, Vorbem. Zu § 7 TMG Rn. 49).

Auch die Rechtsprechung zur Verantwortlichkeit des Registry der Top-Level-Domain .de, der DENIC eG, legt einen weiten Vermittlungs-Begriff zu Grunde:

> *„Der von der Klägerin zur Verfügung gestellte Nameserverdienst gewährleistet die Zuordnung von Domainnamen zu den zugehörigen IP-Adressen des Rechners, von welchem die vom Nutzer durch Eingabe des Domainnamens aufgerufenen Inhalte abzurufen sind. […] Sie vermittelt sonach (im weiteren Sinne) den Zugang zu von Dritten auf Servern vorgehaltenen Informationen."* (VG Düsseldorf, Urteil vom 29.11.2011 - 27 K 458/10).

Sinn- und Zweck des Haftungsausschlusses gem. Art. 12 E-Commerce-Richtlinie bzw. § 8 Abs. 1 TMG gebieten die Anwendung des Haftungsausschlusses auf den Dienst der Antragsgegnerin. Der Haftungsausschluss für reine Durchleitung dient gem. Erwägungsgrund 42 der E-Commerce-Richtlinie dem Schutz von Diensteanbietern, die lediglich eine technische Infrastruktur bereitstellen, über die Informationen, die sie durchleiten oder zu denen sie Zugang vermitteln aber keine Kontrolle haben. Damit soll erreicht werden, dass grundsätzlich gebilligte und technologisch neutrale Diensteanbieter nicht durch übermäßige Haftungsrisiken bedroht werden. Diese teleologischen Erwägungen treffen auf DNS-Resolver zu, deren Geschäftsmodell in der Erbringung einer für das Funktionieren des Internets zentralen, technischen Dienstleistung besteht und die über keine Kontrolle über die Informationen, zu denen Sie Zugang vermitteln, haben. Entsprechend sind DNS-Diensteanbieter – und zwar ausdrücklich neben den Top-Level-Domain Registries – als Betreiber wesentlicher Dienste in Art. 4 Nr. 4 i.V.m. Anhang 2 der NIS-Richtlinie (RL (EU) 2016/1148) genannt. In systematischer Hinsicht wäre es zudem widersprüchlich, wenn Dienste wie DNS-Resolver nicht vom Haftungsausschluss nach § 8 Abs. 1 TMG profitieren könnten und insofern unter verschärfteren Bedingungen als etwa Access Provider, die unstreitig unter den Haftungsausschluss von § 8 Abs. 1 TMG fallen hafteten. DNS-Resolver sind wertungsmäßig von der rechtsverletzenden Information weiter entfernt als Access Provider, da sie die Informationen nicht einmal durchleiten.

Wie bereits dargetan betreiben Access Provider regelmäßig auch rekursive DNS-Resolver. Wollte man den logisch zwingend vorgelagerten Schritt der DNS-Abfrage nicht unter den technischen Lebenssachverhalt des Anbieters eines Telemediendienstes fassen wollen, würde dies dazu führen, dass die Privilegierungen, die maßgeblich durch Zumutbarkeitskriterien motiviert sind, allesamt ins Leere liefen, da die Anbieter sodann zwar nicht in ihrer Eigenschaft als Access Provider, wohl aber in ihrer Eigenschaft als Anbieter eines rekursiven DNS-Resolvers Haftungs- und Prüfungsrisiken ausgesetzt wären.

Dieses Ergebnis wird durch den Entwurf der Europäischen Kommission für eine Verordnung über einen Binnenmarkt für digitale Dienste (Digital Services Act – DSA) und zur Änderung der Richtlinie 2000/31/EG gestützt. Der Europäische Gesetzgeber überführt die Haftungsprivilegierungen der E-Commerce-Richtlinie wortgleich in den DSA. Er Erwägungsgrund 27 des Entwurfs für den DSA stellt klar, dass DNS-Dienste die Haftungsprivilegierungen in Anspruch nehmen können:

> *„Seit dem Jahr 2000 wurden neue Technologien entwickelt, die für eine bessere Verfügbarkeit, Wirksamkeit, Geschwindigkeit, Verlässlichkeit, Kapazität und Sicherheit von Systemen für die Übermittlung und Speicherung von Daten im Internet sorgen, wodurch ein immer komplexeres Online-Ökosystem entstanden ist. In dieser Hinsicht sollte daran erinnert werden, dass Anbieter* ***von Diensten zur Bereitstellung und Vereinfachung der zugrunde liegenden logischen Architektur und des reibungslosen Funktionierens des Internets, einschließlich technischer Hilfsfunktionen****, ebenfalls die in dieser Verordnung festgelegten Haftungsausschlüsse in Anspruch nehmen können, sofern ihre Dienste als „reine Durchleitung", „Caching" oder „Hosting" einzuordnen sind.* ***Zu solchen Diensten gehören*** *gegebenenfalls lokale Funknetze (WLAN)****, DNS-Dienste****, die Dienste von Namenregistern der Domäne oberster Stufe und Zertifizierungsstellen, die digitale Zertifikate ausstellen, oder Netze zur Bereitstellung von Inhalten, die Funktionen anderer Anbieter von Vermittlungsdiensten bereitstellen oder verbessern. Auch Dienste für Kommunikationszwecke und die technischen Mittel für ihre Bereitstellung haben sich stark entwickelt und zur Entstehung von Online-Diensten wie der Internet-Sprachtelefonie (VoIP), Nachrichtenübermittlungsdiensten und webgestützten E-Mail-Diensten geführt, bei denen die Kommunikation über einen Internetzugangsdienst ermöglicht wird. Bei diesen Diensten ist ebenfalls eine Inanspruchnahme der Haftungsausschlüsse möglich, sofern sie als „reine Durchleitung", „Caching" oder „Hosting" einzuordnen sind."* (Hervorhebung des Unterzeichners).

Dieser Vorschlag stellt klar, dass sämtliche Dienste, auch technische Hilfsfunktionen für die Vereinfachung der des Internets zugrunde liegenden logischen Architektur, darunter ausdrücklich DNS-Dienste grundsätzliche eine Haftungsprivilegierung in Anspruch nehmen können. Durch die Formulierung „sollte daran erinnert" werden und die Beibehaltung des Wortlauts der E-Commerce-Richtlinie wird deutlich, dass der Europäische Gesetzgeber in Erwägungsgrund 27 lediglich klarstellt, dass DNS-Diensteanbieter auch unter der geltenden Rechtslage unter den Haftungsausschluss für reine Durchleitung fallen. Zu den privilegierten Diensteanbietern zählen nach Erwägungsgrund 27 auch solche, die technische Hilfsfunktionen anbieten. Die begleitenden Gesetzesmaterialien zum Entwurf für den DSA

machen zudem deutlich, dass der Begriff „DNS-Dienste“ auch rekursive DNS-Resolver einschließt. Die Europäische Kommission bezieht sich in ihrem Inception Impact Assessment für den DSA auf ihren Report zur „Legal analysis of the intermediary service providers of non-hosting nature” (abrufbar unter: https://op.europa.eu/de/publication-detail/-/publication/3931eed8-3e88-11eb-b27b-01aa75ed71a1/language-en/format-PDF/source-179885922), in dem rekursive DNS-Resolver ausdrücklich als Teil der DNS-Dienste erwähnt werden (S. 46).

Der Dienst der Antragsgegnerin erfüllt auch die weiteren Voraussetzungen von § 8 Abs. 1 S. 1 Nr. 1 – 3 TMG, namentlich dass sie die Übermittlung nicht veranlasst, den Adressaten der übermittelten Informationen nicht auswählt und die übermittelten Informationen nicht auswählt oder verändert. Entgegen der Ansicht der Antragstellerin entfällt die Privilegierung nach § 8 Abs. 1 TMG auch nicht deswegen, weil die Antragsgegnerin Filterlisten einsetzt (Antrag, S. 17). Der EuGH hat entschieden, dass der Einsatz freiwilliger Maßnahmen zur Bekämpfung von Rechtsverletzungen durch Diensteanbieter nicht zum Verlust der Haftungsprivilegierungen der E-Commerce-RL führen darf (EuGH, Urt. v. 22.6.2021, C-682/18 und C-683/18 – Youtube/Cyando, Rn. 109). Der EuGH hat in Bezug auf das Hosting-Provider-Privileg gem. Art. 14 E-Commerce-RL klargestellt, dass die freiwillige Anwendung technischer Maßnahmen durch den Diensteanbieter zur Bekämpfung von Rechtsverletzungen nicht dazu führt, dass dieser eine “aktive Rolle” spielt, weil er andernfalls von der Haftungsprivilegierung gem. Art. 14 E-Commerce-RL ausgeschlossen wäre (EuGH a.a.O.). Entsprechend dürfen auch freiwillige technische Maßnahmen zur Bekämpfung von Rechtsverletzungen durch Diensteanbieter gem. § 8 TMG nicht zum Verlust der Haftungsprivilegierung führen.

1.2.3 Anwendbarkeit von § 9 TMG auf Zwischenspeicherung

Soweit die Antragsgegnerin Ergebnisse der rekursiven Namensauflösung zwischenspeichert, ist sie nach § 9 TMG haftungsprivilegiert. Das vorbeschriebene DNS-Caching stellt eine automatische, zeitlich begrenzte Zwischenspeicherung dar, die allein dem Zweck dient, die Übermittlung fremder Anfragen an andere Anfragende effizienter zu gestalten. Die Antragsgegnerin speichert zwar keine Inhalte, sondern auf Anweisung der Anfragenden die DNS-Abfrage-Ergebnisse.

Entgegen der Auffassung der Antragstellerin ist die Haftungsprivilegierung nach § 9 TMG auf den Dienst der Antragsgegnerin auch anwendbar. Die Antragsgegnerin hat weder Kenntnis noch Kontrolle über die bei ihr gespeicherten „Informationen“. Der Umstand, dass die Antragsgegnerin mithilfe der Umsetzung von Sicherheitslisten Schadsoftware aus der DNS-Abfrage filtert, bedeutet nicht, dass sie aktiven Einfluss auf die zwischengespeicherten DNS-Abfrage-Ergebnisse nimmt. Die Antragsgegnerin speichert im Cache die Auflösung einer DNS-Anfrage, die häufig gestellt wird und deshalb ist ihr Verhalten bei der Speicherung technischer, automatischer und passiver Art.

Gemäß § 9 Satz 1 Nr. 5 TMG sind Diensteanbieter für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern sie unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen

Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat. Keine dieser Bedingungen liegt vor.

1.3 Keine Störerhaftung der Antragsgegnerin

Sollte das Gericht ungeachtet der vorstehenden Ausführungen von einer Haftung der Antragsgegnerin ausgehen, so ist gleichwohl keine Störerhaftung gegeben.

1.3.1 Kein adäquat-kausaler Beitrag der Antragsgegnerin zur behaupteten Urheberrechtsverletzung

Die Bereitstellung des Dienstes der Antragsgegnerin stellt keinen adäquat-kausalen Beitrag für die von der Antragstellerin behauptete Urheberrechtsverletzung dar. Die öffentliche Zugänglichmachung ist vorliegend ohne einen Beitrag der Antragsgegnerin vollendet. Die Antragstellerin trägt vor, dass eine öffentliche Zugänglichmachung geschehe, indem unter der beanstandeten Domain durch Hyperlinks auf eine weitere Website das streitgegenständliche Musikalbum zum Download bereitgestellt werde. Der Betrieb des DNS-Resolvers der Antragsgegnerin ist für diese Urheberrechtsverletzung nicht kausal. Denn die öffentliche Zugänglichmachung geschieht durch das Setzen von Hyperlinks auf der beanstandeten Website, bzw. durch das Bereithalten zum Download auf der Drittwebsite. Der Tatbestand der öffentlichen Zugänglichmachung nach § 19a UrhG wird in dem Moment erfüllt, in dem der Schutzgegenstand zum Abruf auf einer Website im Internet bereitgestellt wird. Die maßgebliche Verwertungshandlung ist das Zugänglichmachen eines Schutzgegenstands für den Abruf, die bei Internetsachverhalten u.a. dann verwirklicht ist, sobald der Schutzgegenstand auf einer Website abrufbar ist. Auf den tatsächlichen Abruf des Werkes kommt es nicht an (Wandtke/Bullinger, Urheberrecht, 5. Aufl. 2019, § 19a Rn. 10).

Die Handlung der öffentlichen Zugänglichmachung ist somit unabhängig von tatsächlichen Abrufen bereits in dem Moment vollendet, indem der Schutzgegenstand auf der Website veröffentlicht ist. Die streitgegenständlichen Tonaufnahmen wurden im Moment der Veröffentlichung der Hyperlinks oder der Bereitstellung zum Download abrufbar, und zwar unabhängig von der Nutzung des DNS-Resolvers der Antragsgegnerin. Internetnutzer können über zahlreiche andere DNS-Resolver als den der Antragsgegnerin, etwa über den ihres Internetproviders oder anderer Anbieter auf die Website zugreifen. Die „konkrete Begehungsform“ (Antrag S. 13) ist nicht der Abruf der Tonaufnahmen, sondern deren Bereitstellung. Für die Verwirklichung der öffentlichen Zugänglichmachung ist es nicht erforderlich, dass ein bestimmter DNS-Resolver zur Auflösung des Domainnamens verwendet wird.

Es handelt sich bei der Abrufbarkeit ohne die Nutzung des Dienstes der Antragsgegnerin auch nicht um einen unbeachtlichen hypothetischen Kausalverlauf. Erstens handelt es sich bei dem Beitrag der Antragsgegnerin nicht um das haftungsbegründende Ereignis. Dieses liegt in der Zugänglichmachung auf der beanstandeten Website und tritt ohne einen Beitrag der Antragsgegnerin ein. Der Betrieb ihres DNS-Resolvers kann hinweggedacht werden, ohne dass diese Zugänglichmachung entfiele. Zweitens ist, auch wenn man auf den konkreten Abruf

abstellt, nicht jeder hypothetische Kausalverlauf unbeachtlich. Der BGH stellt in der Entscheidung, auf die er sich in dem Urteil *Störerhaftung des Registrars* beruft, klar, dass die Beachtlichkeit hypothetischer Kausalverläufe eine Wertungsfrage ist, die in verschiedenen Konstellationen unterschiedlich beantwortet wird:

> „Ob die Reserveursache beachtlich ist und zu einer Entlastung des Schädigers führt, ist eine Wertungsfrage, die für verschiedene Fallgruppen durchaus unterschiedlich beantwortet wird (vgl. BGHZ 29, 207, 215; Staudinger/Medicus, BGB 12. Aufl. § 249 Rdnr. 99ff; Larenz, Schuldrecht I 13. Aufl. § 30 I jeweils m.w.N.). Die Erkenntnis, daß eine nur hypothetisch wirksame Reserveursache nicht die Kausalität einer in der Realität wirksam gewordenen Ursache beseitigen kann, beschränkt sich nicht nur auf das Schadensersatzrecht" (BGH, Urt. v. 07.06. 1988, IX ZR 144/87, juris Rn. 12).

Der Beitrag der Antragsgegnerin ist allerdings wertungsmäßig nicht mit dem des Registrars vergleichbar. Anders als der Registrar, der durch die Konnektierung die Erreichbarkeit der Website unter dem Domainnamen überhaupt erst ermöglicht (BGH, GRUR 2021, 63 Rn. 19 – Störerhaftung des Registrars), ist die Website unter dem Domainnamen unter Nutzung jedes beliebigen DNS-Resolvers erreichbar. Anders als die Nutzung eines DNS-Resolvers ist der Beitrag des Registrars nicht beliebig austauschbar und spielt somit eine zentrale Rolle für die Zugänglichmachung.

Schließlich lässt sich, anders als die Antragstellerin meint, auch kein adäquat-kausaler Beitrag der Antragsgegnerin aus der Rechtsprechung des BGH zur Störerhaftung von Access Providern ableiten. Die Antragstellerin gibt die Entscheidung des BGH zur Störerhaftung des Access Providers nur unvollständig wieder. In der von der Antragstellerin in Bezug genommenen Randnummer 25 der Entscheidung *Störerhaftung des Access Providers* hat der BGH festgestellt:

> „Durch die Vermittlung des Zugangs hat die Beklagte nach der zutreffenden Beurteilung des Berufungsgerichts einen adäquat kausalen Beitrag zu der vom Berufungsgericht festgestellten Urheberrechtsverletzung geleistet. Nach dem Erwägungsgrund 59 der RL 2001/29/EG bezieht sich der in der Richtlinie verwendete Begriff des „Vermittlers" auf jede Person, die die Rechtsverletzung eines Dritten in Bezug auf ein geschütztes Werk in einem Netz übertragt. Zur Rechtsverletzung in diesem Sinne zählt das öffentliche Zugänglichmachen eines Schutzgegenstands (EuGH, GRUR 2014, 468 Rn. 31 – UPC Telekabel). Da der Anbieter von Internetzugangsdiensten durch die Gewährung des Netzzugangs die Übertragung einer solchen Rechtsverletzung im Internet zwischen seinem Kunden und einem Dritten möglich macht, ist der Diensteanbieter an jeder Übertragung zwingend beteiligt, so dass seine Zugangsdienste iSd Art. 8 III RL 2001/29/EG zu einer Urheberrechtsverletzung genutzt werden (vgl. EuGH, GRUR 2014, 468 Rn. 32, 40 – UPC Telekabel)." (BGH GRUR 2016, 268 Rn. 25 – Störerhaftung des Access-Providers)

Der BGH stellt damit klar, dass der Beitrag des Access Providers deswegen adäquat-kausal war, weil der Access Provider an der Übertragung rechtswidriger Inhalte in seinem Netz

zwingend beteiligt ist. Dies ist bei dem Dienst der Antragsgegnerin nicht der Fall. Die Antragsgegnerin ist nicht, erst recht nicht zwingend, an der Übertragung rechtswidriger Informationen beteiligt. Die öffentliche Zugänglichmachung durch das Setzen von Hyperlinks bzw. die Herstellung der Abrufbarkeit wird unabhängig von der Nutzung des Dienstes der Antragsgegnerin vollendet (s.o.). Die Antragstellerin überträgt die so öffentlich zugänglich gemachten Tonaufnahmen auch nicht an Dritte. Ihr Dienst besteht lediglich in der Beantwortung der DNS-Anfragen.

Schließlich ist es widersprüchlich, wenn die Antragstellerin einerseits darlegt, der Tatbeitrag der Antragsgegnerin bestehe – gleich dem eines Access Providers – darin, dass sie den Zugang zu einem Netz herstellt, das eine Übertragung ermögliche und andererseits der Antragsgegnerin die Haftungsprivilegierung nach § 8 Abs. 1 S. 2 TMG absprechen will, die an eben jene Handlung geknüpft ist.

1.3.2 Keine Verletzung zumutbarer Prüfpflichten

Die Antragsgegnerin erfüllt den Tatbestand der Störerhaftung nicht, da sie keine zumutbaren Prüfpflichten verletzt hat. Die Störerhaftung für als rechtsverletzend beanstandete Inhalte im Internet unterliegt nach der Rechtsprechung des BGH je nach Ausgestaltung von Funktion und Tätigkeit des Inanspruchgenommenen unterschiedlichen Anforderungen (BGH, Urteil v. 15.10.2020, I ZR 13/19, Rn. 21). Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden kann, die die rechtswidrige Beeinträchtigung nicht selbst vorgenommen haben, setzt die Haftung des Störers die Verletzung von Verhaltenspflichten voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist (BGH, a.a.O, Rn. 13).

Grundsätzlich treffen die Antragsgegnerin keine Prüf- und Überwachungspflichten in Bezug auf die Informationen, zu denen sie den Zugang vermittelt. Nach der Rechtsprechung des BGHs entstehen Prüf- und Überwachungspflichten für die Betreiber technische neutraler Internetdienste regelmäßig erst nach einem Hinweis auf eine konkrete Rechtsverletzung (zusammenfassend für Registries, Admin-C, Host-Provider, Access Provider und Registrar: BGH, a.a.O., Rn. 22 ff.). An die Substantiierung und Bestimmtheit des Hinweises auf die Rechtsverletzung gelten wiederum gestaffelte Anforderungen, die sich unter anderem danach richten, ob die Tätigkeit des jeweiligen Diensteanbieters im Allgemeininteresse liegt, ob sie mit Gewinnerzielungsabsicht erbracht wird, ob sie mit einer Speicherung der rechtswidrigen Informationen verbunden ist, ob die effiziente Erfüllung der Aufgaben durch die rechtliche Prüfung des Hinweises beeinträchtigt wird und ob es tatnähere Beteiligte gibt (BGH, a.a.O., Rn. 22 ff., 29). Für die DENIC eG hat der BGH entschieden, dass diese auch bei einem Hinweis auf eine Rechtsverletzung nur eingeschränkte Prüfungspflichten träfen. Nur bei Rechtsverletzungen, die unschwer erkennbar sind, weil sie entweder durch rechtskräftigen gerichtlichen Titel belegt sind oder die Verletzung derart eindeutig ist, dass sie sich ohne Nachforschungen aufdrängen muss, erwachsen der DENIC eG demnach konkrete Prüfpflichten. Das Pflichtenprogramm der DENIC eG ist nach der Rechtsprechung des BGH auf diese besonders substantiierten Hinweise beschränkt, weil sie unentgeltlich eine im Allgemeininteresse liegende Aufgabe erbringt (BGH, a.a.O. Rn. 22). Demgegenüber unterliegt die Haftung des Registrars weniger strengen Anforderungen, da dieser durch die Abwicklung

der Domain-Registrierung zwar eine Aufgabe im Allgemeininteresse erfülle, dabei jedoch mit Gewinnerzielungsabsicht handele. Daher genügt im Falle des Registrars der Hinweis auf eine klare und ohne weiteres feststellbare Rechtsverletzung, um Prüfpflichten auszulösen (BGH, a.a.O. Rn. 28 - 30.). In jedem Fall muss der Hinweis sämtliche Anspruchsvoraussetzungen enthalten (BGH, a.a.O. Rn. 35). Die Anforderungen an den Hinweis bei Registrar und nicht-kommerzieller Registry unterscheiden sich nach der Rechtsprechung des BGH bezüglich der Anforderungen an die Erkennbarkeit des Vorliegens der Anspruchsvoraussetzungen. Für den kommerziell handelnden Registrar muss die Rechtsverletzung klar und ohne weiteres feststellbar sein, für die nicht-kommerzielle Registry ist der Maßstab demgegenüber so verschärft, dass die Rechtsverletzung entweder aus einem rechtskräftigen Titel hervorgehen oder sich aufdrängen muss.

Für die Antragsgegnerin kann kein weniger strenger Maßstab als für die DENIC eG gelten. Die Antragsgegnerin wirkt an einer Aufgabe im Allgemeininteresse mit, da sie zum reibungslosen Ablauf von DNS-Anfragen beiträgt. Sie erbringt diese Dienstleistung unentgeltlich und bietet ihren Nutzern einen Schutz vor schädlicher Software unter Einhaltung geltender Datenschutzvorschriften und Wahrung der Privatsphäre der Nutzer. Ebenso wie die DENIC eG erbringt die Antragsgegnerin eine rein technische, inhaltlich neutrale Aufgabe. An die Prüfpflichten der Antragsgegnerin müssen gegenüber der DENIC eG verschärfte Anforderungen gelten, auch deshalb, weil die DENIC eG „lediglich" Domains unter der Endung „.de" in ihrer Verwaltung hat, während die Antragsgegnerin DNS-Abfragen zu Tausenden von Top Level Domains bearbeitet und Hunderte von Millionen von Domains betroffen sein können.

Eine Prüfpflicht der Antragsgegnerin kann ausschließlich durch Hinweise auf Grundlage eines rechtskräftigen Titels oder bei solchen Rechtsverletzungen entstehen, bei der die Natur der geltend gemachten Rechtsverletzung aus dem Inhalt selbst ersichtlich ist. Wie im Hinblick auf die von der Antragsgegnerin eingesetzten Filterlisten kann von einer offensichtlichen, sich aufdrängenden Rechtsverletzung in diesem Kontext nur ausgegangen werden, wenn es sich um generell, global unerwünschte und dem Inhalt immanente Verletzungen und Inhalte handelt. Die Sperrlisten betreffen Malware, Viren, Botnets, Phishing-Seiten, Stalkerware und andere Arten von Inhalten, die global rechtswidrig sind. Hier besteht kein Deutungs- oder Gestaltungsspielraum. Demgegenüber sind Rechtsverletzungen, die von behaupteten Rechteinhaberdarstellungen, mangelnder Lizenzierung oder ähnlichen Umständen abhängen, die der Privatautonomie und Vertragsgestaltung der jeweiligen Parteien unterliegen, für die Antragsgegnerin nicht ersichtlich und nicht zumutbar dahingehend prüfbar, ob gegebenenfalls doch eine Berechtigung des angeblichen Rechtsverletzers gegeben ist.

Soweit die von der Antragstellerin verlangte Maßnahme dazu führt, dass eine Domain weltweit nicht mehr erreichbar ist, müsste die Antragsgegnerin durch den Hinweis in die Lage versetzt werden, die Voraussetzungen der Sperrung einer Information in allen betroffenen Jurisdiktionen festzustellen. Andernfalls wäre die Antragsgegnerin zu einer derart aufwändigen juristischen Prüfung gezwungen, ihr die Aufgabenerfüllung unmöglich machen würde. Dazu kommt das Erfordernis, die Identität der jeweiligen Anspruchsteller zu prüfen, um Sperrungsbegehren seitens unberechtigter Parteien zu vermeiden.

Auch wenn man den Maßstab, den der BGH für die DENIC eG entwickelt hat, anwendet und Prüfpflichten der Antragsgegnerin unter der Voraussetzung annimmt, dass sie einen Hinweis erhält, der es ihr ermöglicht, eine Rechtsverletzung ohne weitere Nachforschungen festzustellen, etwa durch einen rechtskräftigen gerichtlichen Titel oder weil die Rechtswidrigkeit aus dem Inhalt selbst heraus erkennbar ist, kommt eine Verletzung von Prüfpflichten vorliegend nicht in Betracht.

1.3.2.1 Kein Zugang des Hinweises auf die behauptete Rechtsverletzung

Die Antragsgegnerin wurde von der Antragstellerin nicht auf die Umstände hingewiesen, weil der Verfahrensbevollmächtigte der Antragstellerin weder das Hinweisschreiben noch die Abmahnschreiben ordnungsgemäß an die Antragsgegnerin übersandte. Ein Zugang, für den die Antragstellerin darlegungs- und beweisbelastet ist, liegt nicht vor. Bei dem Versand per E-Mail trägt die Antragstellerin die Beweislast für den ordnungsgemäßen Zugang sowohl des Hinweis- als auch eines Abmahnschreibens. Das Risiko des tatsächlichen Zugangs im Postfach der Antragsgegnerin trägt die Antragstellerin. Wenn eine E-Mail bereits vom Spam-Filter des Servers aussortiert wird, geht dieses Risiko zu Lasten des Absenders (Wandtke/Bullinger, Urheberrecht, 5. Aufl. 2019, § 97a Rn. 27). Wenn die E-Mail im lokalen Spam-Ordner eingeht, besteht für den Empfänger keine Pflicht, Anhänge zu öffnen, da damit der Verdacht eines Virenbefalls der Anhänge begründet sein kann (Wandtke/Bullinger, a.a.O.).

Die der E-Mail vom 26.03.2021 beigefügten Anhänge im .pdf-Format wurden von der Antragsgegnerin nicht geöffnet, da üblich ist und empfohlen wird, aus Sicherheitsgründen Anhänge von Mails unbekannter Absender nicht zu öffnen (s.o. 2.7.2.1).

Die Angaben in der Fußzeile führen nicht dazu, dass bei der Antragsgegnerin der Eindruck entstehen musste, dass es sich nicht um Spam handele. Anders als vom BSI empfohlen (s.o.) enthielt die Mail einen sehr kurzen Text ohne Ansprache, Grußformel oder Informationen über den Inhalt der Anhänge.

Der Gesamteindruck der E-Mail stand mithin im Widerspruch zu einer E-Mail in rechtlichen Angelegenheiten, die bei einer Abmahnung erwartet werden kann.

Da die Antragstellerin sowohl außergerichtliche als auch gerichtliche Erfahrungen mit derartigen Verfahren besitzt, ist es ihr zudem zumutbar, eine Abuse-Meldung an die entsprechende E-Mail-Adresse zu adressieren. Der Antragsgegnerin ist nicht zuzumuten und es kann auch nicht von ihr verlangt werden, dass jedwede eingehende E-Mail ohne die Verwendung von technischen Hilfsmitteln zur Eindämmung von Spam und E-Mails mit Schadcode in Augenschein genommen werden muss. Dieses Risiko muss die Antragsgegnerin erst recht nicht bei einer Support-E-Mail-Adresse eingehen, deren Sinn und Zweck die Beantwortung von Fragen zum System ist.

Das nach dem Vortrag der Antragstellerin mit einfacher Post versandte Abmahnschreiben ist der Antragsgegnerin ebenfalls nicht zugegangen. Wenn sich die Antragstellerin zur Beförderung des Abmahnschreibens der Post bedient, wird diese insoweit als Erfüllungsgehilfin der Antragstellerin tätig, sodass in einem solchen Fall die Antragstellerin ein

Verschulden der Post gemäß § 278 Satz 1 BGB zu vertreten hat, wenn auf dem Postweg Postverluste auftreten (vgl. BGH, Urteil v. 21.01.2009 - VIII ZR 107/08).

Ferner ist fraglich, wieso das Hinweisschreiben lediglich per E-Mail und das Abmahnschreiben per Post versandt wurde. Hätte die Antragstellerin Sorge für den Zugang der Schreiben tragen wollen, so hätte sie ein Einwurfeinschreiben oder eine E-Mail mit Lesebestätigung versenden können. Die so entstandenen Unsicherheiten muss sich die Antragstellerin zurechnen lassen, da sie in ihre Risikosphäre fallen.

Die Antragsgegnerin erlangte erstmalig durch die Beschlussverfügung Kenntnis von der geltend gemachten Rechtsverletzung. Sie reagierte daraufhin in einem angemessenen Zeitraum, ohne Anerkennung einer Rechtspflicht, mit der Sperrung der Domain.

1.3.2.2 Kein hinreichend substantiierter Hinweis

Unterstellt, der Antragsgegnerin wären das Hinweis- oder das Abmahnschreiben zugegangen, würden diese keinen hinreichend substantiierten Hinweis auf eine Rechtsverletzung enthalten, der es der Antragsgegnerin ermöglicht hätte, ohne Nachforschungen zweifelsfrei festzustellen, dass aufgrund der von der Antragstellerin geltend gemachten Rechtsverletzung die Sperrung der gesamten Domain [redacted] rechtlich zulässig und geboten wäre. Ein Hinweis, der Prüfpflichten der Antragsgegnerin auszulösen geeignet ist, muss sämtliche Informationen enthalten, die die Antragsgegnerin in die Lage versetzen, die Rechtmäßigkeit des Sperrverlangens ohne nähere Prüfung und zweifelsfrei nachzuvollziehen. Es genügt daher nicht, dass die Antragstellerin eine einzelne Rechtsverletzung plausibel macht, sie muss die Voraussetzungen für die geltend gemachte Sperre der gesamten Domain darlegen.

Dazu zählen insbesondere Hinweise auf den Umstand, dass die beanstandete Domain weit überwiegend rechtsverletzende Inhalte enthält und der Rechtsinhaber erfolglos gegen tatnähere Beteiligte vorgegangen ist (BGH, Urt. vom 15.10.2020, I ZR 13/19, Rn. 35). Nach der Rechtsprechung des BGH kommt eine DNS-Sperre nur dann in Betracht, wenn rechtmäßige Inhalte im Gesamtverhältnis zu den rechtswidrigen Inhalten auf der jeweiligen Website nicht ins Gewicht fallen (BGH a.a.O.). Zudem kommt eine Sperrpflicht erst dann in Betracht, wenn der Rechteinhaber zuvor erfolglos gegen tatnähere Beteiligte vorgegangen ist, einschließlich zumutbarer Maßnahmen zur Aufdeckung der Identität des Betreibers der Website durch Einschaltung staatlicher Ermittlungsbehörden oder privater Ermittler (BGH GRUR 2016, 268, 275, Rn. 87 – Störerhaftung des Access Providers).

Diesen Anforderungen genügen die Informationen aus dem Hinweis- und Abmahnschreiben (Anlagen AST 4 und AST 6) nicht. Das Hinweisschreiben enthält keine Informationen über das erfolglose Vorgehen der Antragstellerin gegen tatnähere Beteiligte und kann diese Informationen auch nicht enthalten, da die Antragstellerin ausweislich des Abmahnschreibens zeitgleich mit dem Versand des Hinweisschreibens am 23.03.2021 sich erstmals an die Betreiber der beanstandeten Domain und ihren Hostprovider gewendet hat.

Die Antragstellerin hat ferner nicht hinreichend substantiiert zum Gesamtverhältnis zwischen rechtmäßigen und rechtsverletzenden Inhalten der beanstandeten Domain vorgetragen. Weder hat sie einen gerichtlichen Titel noch einen vergleichbaren Hinweis, aus dem sich der

Antragsgegnerin die Rechtswidrigkeit der Information ohne Nachforschungen hätte aufdrängen müssen, vorgelegt. Weder die Empfehlung des Prüfungsausschusses noch das Gutachten (Anlage AST 2 und AST 16) waren den Schreiben ordnungsgemäß beigefügt. Die Antragsgegnerin kann sich auf Grundlage dieser Erwähnung der Rechtsverletzung nicht mit der erforderlichen Sicherheit vergewissern. Die Antragsgegnerin hätte nicht nachvollziehen können, ob die Ergebnisse dieser Untersuchung zutreffen oder ob sie überhaupt durchgeführt wurde.

Auch das Gutachten (Anlage AST 6) und die Empfehlung des Prüfungsausschusses (Anlage AST 16) genügen den Substantiierungsanforderungen nicht. Weder das Gutachten noch die Empfehlung des Prüfungsausschusses sind Dokumente, die von einer staatlich anerkannten Stelle stammen, deren Beurteilung mit einem Urteil oder einer Beschlussverfügung gleichzusetzen sind. Das Gutachten lässt außer Betracht, dass die begutachtete Website neben Links auch ein Diskussionsforum enthält, das zahlreiche rechtmäßige Inhalte enthält. Daher ist fraglich, ob angesichts der großen Zahl der verfügbaren Inhalte die sehr kleine Stichprobe von 80 Inhalten überhaupt aussagekräftig sein kann. Die Empfehlung des Prüfungsausschusses lässt sich durch die Antragsgegnerin nicht nachvollziehen, da der Analysebericht, auf das sich die Empfehlung bezieht, der Empfehlung nicht beigefügt ist. Die Empfehlung legt ferner nicht dar, wie weit und warum der Prüfausschuss der Methodik des statistischen Analyseberichts folgt.

Die Antragstellerin hat schließlich auch im Abmahnschreiben keine hinreichend substantiierten Informationen über die Inanspruchnahme tatnäherer Beteiligter vorgetragen. Denn die Antragstellerin legt unabhängig von den weiteren unten adressierten Defiziten jedenfalls nicht dar, dass sie die nach der Rechtsprechung des BGH erforderlichen, zumutbaren Maßnahmen zur Ermittlung der Identität der Betreiber der Website unternommen habe. Sie legt insbesondere nicht dar, dass sie staatliche oder private Ermittlungen eingeleitet habe. Selbst wenn die Antragsgegnerin in eine rechtliche Prüfung eintritt, hätte sie also nicht mit der erforderlichen Sicherheit feststellen können, dass die Subsidiarität ihrer Inanspruchnahme gegenüber den tatnäheren Beteiligten gewährleistet war.

1.3.3 Inanspruchnahme der Antragsgegnerin wegen Subsidiarität ausgeschlossen

Die Inanspruchnahme der Antragsgegnerin ist vorliegend unter dem Gesichtspunkt der Subsidiarität ausgeschlossen. Die Antragstellerin hat nicht glaubhaft gemacht, dass sie alle zumutbaren Anstrengungen unternommen habe, um gegen den Täter der Rechtsverletzung oder sonstige tatnähere Beteiligte vorzugehen.

Die Inanspruchnahme als Störer ist grundsätzlich nicht subsidiär gegenüber der täterschaftlichen Haftung, sofern die Störerhaftung effektiveren Rechtsschutz bietet, weil nicht gegen eine Vielzahl von Rechtsverletzern vorgegangen werden muss (BGH GRUR 2007, 724 Rn. 13). Dies ist vorliegend nicht der Fall. Die Antragstellerin hätte zur Beendigung der öffentlichen Wiedergabe der streitgegenständlichen Tonaufnahmen lediglich einen der tatnäheren Beteiligten in Anspruch nehmen müssen, um die Rechtsverletzung zu beenden.

Nach der Rechtsprechung des BGH ist daher auch die Störerhaftung des Access Providers aus Zumutbarkeitserwägungen subsidiär zur Inanspruchnahme tatnäherer Beteiligter:

> „Im Hinblick darauf, dass der Access-Provider ein von der Rechtsordnung gebilligtes und in Bezug auf Rechtsverletzungen Dritter neutrales Geschäftsmodell verfolgt, ist es im Rahmen der Prüfung der Zumutbarkeit von Überwachungs- und Sperrmaßnahmen angemessen, eine vorrangige Rechtsverfolgung gegenüber denjenigen Beteiligten zu verlangen, die – wie die Betreiber beanstandeter Webseiten – entweder die Rechtsverletzung selbst begangen oder zu der Rechtsverletzung – wie der Host-Provider der beanstandeten Webseiten – durch die Erbringung von Dienstleistungen beigetragen haben. Dagegen kommt die Geltendmachung von Ansprüchen gegen den Zugangsvermittler unter dem Gesichtspunkt der Verhältnismäßigkeit nur in Betracht, wenn der Inanspruchnahme des Betreibers der Webseite jede Erfolgsaussicht fehlt und deshalb andernfalls eine Rechtsschutzlücke entstünde. Für dieses Ergebnis spricht auch der Umstand, dass der Betreiber der Webseite und sein Host-Provider wesentlich näher an der Rechtsgutsverletzung sind als derjenige, der nur allgemein den Zugang zum Internet vermittelt." (BGH, GRUR 2016, 268 Rn. 83 – Störerhaftung des Access Providers)

Dementsprechend hat der BGH entschieden, dass auch der Registrar nur subsidiär als Störer in Anspruch genommen werden könne, die Störerhaftung mit anderen Worten ultima ratio sei:

> „Bei der Abwägung der beteiligten Grundrechte (dazu Rn. 26) ist der Gefahr, dass hieraus eine unverhältnismäßige Belastung des Registrars und damit eine Gefährdung seines Geschäftsmodells folgt, durch die Annahme seiner lediglich subsidiären Haftung Rechnung zu tragen, die erst eintritt, wenn der Rechtsinhaber erfolglos gegen diejenigen Beteiligten vorgegangen ist, die - wie der Betreiber der Internetseite - die Rechtsverletzung selbst begangen haben oder - wie der Host-Provider - zur Rechtsverletzung durch die Erbringung von Dienstleistungen beigetragen haben, sofern nicht einem solchen Vorgehen jede Erfolgsaussicht fehlt. Die Haftung des Registrars ist ebenso wie diejenige des Internetzugangsvermittlers ultima ratio, wenn auf andere Weise der Urheberrechtschutz nicht effektiv sichergestellt werden kann (vgl. BGHZ 208, 82 Rn. 83 - Störerhaftung des Accessproviders)." (BGH, Urt. vom 15.10.2020, I ZR 13/19, Rn. 31 – Störerhaftung des Registrars)

Diese Haftungsgrundsätze sind auf den DNS-Resolver zu übertragen. Auch die Antragsgegnerin betreibt mit der Vermittlung des Zugangs zum Internet ein von der Rechtsordnung gebilligtes, gesellschaftlich und in Bezug auf Urheberrechtsverletzungen Dritter neutrales Geschäftsmodell. Wie der Access Provider hat auch die Antragsgegnerin keine vertraglichen Beziehungen zu tatnäheren Beteiligten wie dem Betreiber der beanstandeten Website oder dessen Host-Provider.

Die Antragstellerin hat nicht glaubhaft gemacht, dass sie zumutbare Maßnahmen zur Inanspruchnahme der tatnäheren Beteiligten ergriffen hat.

1.3.3.1 Antragstellerin hat zumutbare Maßnahmen zur Ermittlung der Identität des Website-Betreibers nicht ausgeschöpft

Die Antragstellerin hat nicht sämtliche ihr zumutbare Maßnahmen zur Ermittlung der Identität der Betreiber der beanstandeten Website ergriffen. Nach der Rechtsprechung des BGH ist dem Rechtsinhaber in diesem Zusammenhang insbesondere die Einschaltung staatlicher Ermittlungsbehörden oder die Vornahme privater Ermittlungen zumutbar. Allein dass die Identität des Website-Betreibers nicht aus der Website entnommen werden kann, entbindet den Rechtsinhaber nicht von der Ergreifung weiterer Maßnahmen (BGH, GRUR 2016, 268 Rn. 87 – Störerhaftung des Access Providers). Diesen Anforderungen hat die Antragstellerin nicht genügt. Sie hat insbesondere nicht dargelegt, staatliche Ermittlungsbehörden oder private Ermittler eingeschaltet zu haben. Die Antragstellerin trägt vor, dass die beanstandete Website kein Impressum habe, es keinen öffentlichen Whois-Eintrag geben und die Betreiber auf eine Nachricht an den Administrator des Forums der Website nicht reagiert hätten. Dass die Identität der Betreiber sich über die Website nicht ermitteln ließ, ist nach vorgenannter Entscheidung des BGH nicht ausreichend. Das Fehlen eines Whois-Eintrags entbindet nicht von dem Ergreifen weiterer Maßnahmen. Die Domain, die der BGH-Entscheidung zur Störerhaftung des Access Providers zugrunde liegt, goldesel.to, und die vorliegend beanstandete Domain teilen die Top-Level-Domain .to. Der BGH hielt also auch unter der Voraussetzung, dass die entsprechende Top-Level-Domain nicht über ein öffentliches Whois-Verzeichnis verfügt, die Ergreifung weiterer Maßnahmen für zumutbar.

Die Antragstellerin ist auch nicht der zumutbaren Einschaltung staatlicher oder privater Ermittlungen entbunden, weil sie sich per E-Mail an den Werbevermarkter [redacted] oder den Zahlungsdienstleister [redacted] gewendet hat. Der BGH nennt den Ermittlungsansatz über Zahlungsdienstleister ausdrücklich als selbstständige Maßnahme neben der Einleitung von Ermittlungen (BGH a.a.O.).

Die Auskunftsersuchen, die die Antragstellerin an die o.g. Dienstleister gerichtet hat, stellen zudem keinen geeigneten Versuch dar, die Identität der Betreiber der beanstandeten Website zu ermitteln. Die Antragstellerin hat nicht dargelegt, auf welchem Kommunikationsweg sie versucht hat, die Anwaltsschreiben (Anlagen AST 8 und AST 9) zuzustellen. Insofern wird bestritten, dass die Anwaltsschreiben den jeweiligen Diensten zugegangen sind. Zudem sind die Formulierungen in den Anwaltsschreiben nicht hinreichend deutlich und zum Teil widersprüchlich. In beiden Anwaltsschreiben wird darauf Bezug genommen, dass die Dienste in Geschäftsbeziehungen zu der Website [redacted] stünden. Als Beleg für die Verletzung von Rechten der Antragstellerin werden jedoch ausschließlich URLs unter einer anderen Domain, [redacted], angeführt. Eine Aktivlegitimation legt die Antragstellerin nicht dar, nicht einmal eine schriftliche Anwaltsvollmacht war den Schreiben beigefügt. Im Rubrum der Schreiben ist keine vollständige Adresse der Antragstellerin angegeben. Schon insoweit dürfte es den Diensten nicht möglich gewesen sein, die Authentizität des Auskunftsersuchens der Antragstellerin nachzuvollziehen.

Mit dem Schreiben an [redacted] (Anlage AST 8) fordert die Antragstellerin den Dienst [redacted] zudem auf, das Schalten von Werbung unter der Domain [redacted] zu beenden. Dies steht nicht nur im Widerspruch zu den zuvor aufgeführten Rechtsverletzungen, die sich

auf eine andere Domain beziehen, dieses Verlangen geht auch deutlich über ein Auskunftsersuchen hinaus. Die Antragstellerin legt nicht dar, auf welche Rechtsgrundlage sie vermeintliche Unterlassungs- oder Auskunftsansprüche stützt. Der Dienst [redacted] kann das Schreiben daher nicht so verstehen, dass er auf Grundlage dieser spärlichen und widersprüchlichen Informationen zur Herausgabe personenbezogener Daten, geschweige denn zur Beendigung vertraglicher Beziehungen, die entsprechende Regressansprüche begründen kann, verpflichtet sein sollte. In dem Schreiben an [redacted] legt die Antragstellerin ebenfalls keine Rechtsgrundlage für ihr Auskunftsersuchen dar. Sie bezieht ihr Auskunftsersuchen allein auf die Domain [redacted]. Ohne weitere Informationen kann der Zahlungsdienstleister diesen Anspruch jedoch nicht einmal einem Spendenkonto zuordnen. Die Antragstellerin hätte zumindest den Account, auf den sich das Auskunftsersuchen bezieht, benennen müssen. Auch [redacted] kann auf Grundlage dieses Auskunftsschreibens daher nicht ernsthaft von einer Auskunftspflicht ausgegangen sein.

Beide Schreiben sehen zudem eine Frist von drei Tagen vor, um die geltend gemachten Ansprüche zu erfüllen. Zu den bereits dargelegten Substantiierungsmängeln, Widersprüchen und Unklarheiten bei der Zustellung kommt hinzu, dass der Verfahrensbevollmächtigte der Antragstellerin mit den Anwaltsschreiben die Rechte weiterer Rechteinhaber an zahlreichen anderen Werken geltend macht. Diesbezüglich sind die Schreiben in weiteren Aspekten widersprüchlich (einige Alben werden mehrfach angegeben) und die Frist zudem so kurz, dass die tatsächliche und rechtliche Überprüfung innerhalb dieser Frist faktisch unmöglich ist. Nach alldem konnten die Dienstleister nicht davon ausgehen, zur Erteilung von Auskünften verpflichtet zu sein.

1.3.3.2 Antragstellerin hat zumutbare Maßnahmen zur Inanspruchnahme des Host-Providers nicht ausgeschöpft

Die Antragstellerin hat auch nicht sämtliche zumutbaren Maßnahmen ergriffen, um die Rechtsverletzung durch Inanspruchnahme des Host-Providers der beanstandeten Domain zu beenden. Das als Anlage AST 10 vorgelegte Anwaltsschreiben der Antragstellerin war ebenfalls nicht hinreichend substantiiert, sodass auch der Host-Provider nicht von einer Löschpflicht ausgehen musste. Die Antragstellerin hat auch hier ihre Aktivlegitimation nicht dargelegt. In dem Rubrum dieses Anwaltsschreiben fehlt ebenfalls eine vollständige Adresse der Antragstellerin, ebenso wie eine schriftliche Vollmacht des Verfahrensbevollmächtigten der Antragstellerin. In der Gesamtschau wirkt das Schreiben für einen objektiven Empfänger nicht als wirksame Aufforderung zur Beendigung eines Vertragsverhältnis mit den Betreibern der beanstandeten Website. Zu den Substantiierungsmängeln treten erneut Widersprüche hinzu, die den Eindruck der Ernsthaftigkeit in Frage stellen. Das Schreiben nennt keine Rechtsgrundlage für die behaupteten Ansprüche. Es werden mehrere Alben ohne erkennbaren Grund doppelt aufgeführt. Das Schreiben enthält ferner Übersetzungsfehler, z.B. ist die Vertretung der [redacted] auf Deutsch formuliert. Ohne weitere Informationen seitens der Antragstellerin kann der Host-Provider nicht davon ausgehen, zur Beendigung seiner Dienstleistung gegenüber den Betreibern der beanstandeten Website verpflichtet zu sein.

1.3.3.3 Keine Ermittlung eines tatnäheren Registrars

Wenngleich Tonic Domainregistrierungen unmittelbar gegenüber ihren Kunden anbietet, hätte die Antragstellerin darlegen müssen, dass die Domain ohne Einschaltung eines Registrars registriert wurde und eine Inanspruchnahme des Registrars damit nicht in Betracht kam. Dies liegt in dem Umstand, dass zumeist Domainregistrierungen über Registrare erfolgen und Registrare der Rechtsverletzung näher sind. Einerseits steht der Registrar in einem Vertragsverhältnis mit dem Domain-Betreiber. Er steht mangels Kenntnis der Inhalte der Website die er konnektiert zwar nicht im Lager des Website-Betreibers, gleichwohl ist er diesem durch eine vertragliche Beziehung verbunden. Dies ist bei der Antragsgegnerin, die eine vollständig technische neutrale Dienstleistung erbringt, nicht der Fall. Andererseits handelt der Registrar mit Gewinnerzielungsabsicht, sodass ihm auch insoweit größere Verpflichtungen als der nicht-kommerziell handelnden Antragsgegnerin zumutbar sind. Die Beendigung der Rechtsverletzung durch den Registrar ist zudem effektiver als die Blockierung durch den DNS-Resolver der Antragsgegnerin. Die dem Registrar mögliche Dekonnektierung der beanstandeten Domains erfordert nicht, dass technische Maßnahmen in eine empfindliche Infrastruktur installiert und regelmäßig aktualisiert werden, sondern nur einen administrativen Schritt. Die Dekonnektierung berührt ausschließlich die Adressierbarkeit über die Domain, beseitigt diese aber vollständig. Sie ist insofern effektiver als eine DNS-Sperre durch die Antragsgegnerin, die in den meisten Fällen wegen der automatisierten Nutzung alternativer DNS-Resolver wirkungslos ist und mit dem nötigen technischen Wissen durch Umwege über andere DNS-Resolver umgangen werden kann.

Informationen zur erfolgten erfolglosen Inanspruchnahme des Registrars oder zum Fehlen eines Registrars wären insofern für einen wirksamen Hinweis an die Antragsgegnerin erforderlich gewesen.

1.3.4 Störerhaftung der Antragsgegnerin wegen Unverhältnismäßigkeit ausgeschlossen

Die Haftungsgrundsätze, die EuGH und BGH im Zusammenhang mit Access Providern entwickelt haben und die der BGH auch auf den Registrar anwendet, sind auf DNS-Resolver zu übertragen. Die DNS-Sperre durch den DNS-Resolver folgt derselben Logik wie die Sperrung durch den Access-Provider, die dieser Ebenfalls durch eine Konfiguration des DNS-Resolvers vornimmt. Die Dienstleistung des DNS-Resolvers ist ebenfalls technisch neutral, anders als Registrar oder Access Provider erbringt die Antragsgegnerin diese Dienstleistung vorliegend sogar unentgeltlich. Nach der Rechtsprechung des EuGH ist bei der Beurteilung, ob gerichtliche Verfügungen gegen Zugangsanbieter mit dem Unionsrecht im Einklang stehen, die Vereinbarkeit mit den betroffenen Grundrechten der EU-Grundrechtecharta (GrCh) zu prüfen (EuGH, GRUR 2014, 468 Rn. 45 f. – UPC Telekabel). Das nationale Recht ist daher unter Beachtung der Grundrechte der Charta und des Verhältnismäßigkeitsgrundsatzes anzuwenden (BGH, GRUR 2016, 268 Rn. 31 – Störerhaftung des Access Providers).

1.3.4.1 Mangelnde Zielgerichtetheit

Die vom Gericht angeordnete Maßnahme ist unverhältnismäßig, da sie nicht den Anforderungen an die Zielgerichtetheit genügt.

1.3.4.1.1 Keine gerichtlichen Rechtsschutzmöglichkeiten

Die Inanspruchnahme der Antragsgegnerin als Störerin stellt einen unverhältnismäßigen Eingriff in die Informationsfreiheit der betroffenen Nutzer dar, da den Nutzern der Antragsgegnerin keine gerichtlichen Rechtschutzmöglichkeiten offenstehen.

Nach der Rechtsprechung des EuGH setzt die Rechtmäßigkeit der Anordnung einer Website-Sperre unter dem Aspekt der Informationsfreiheit voraus, dass die nationalen Verfahrensvorschriften den Internetnutzern ermöglichen, ihre Recht nach Bekanntwerden der vom Anbieter getroffenen Sperrmaßnahmen vor Gericht geltend zu machen (EuGH, GRUR 2014, 468 Rn. 56 – UPC Telekabel). Dem hat sich der BGH angeschlossen und in Bezug auf Website-Sperren durch den Access Provider klargestellt, dass das nationale Recht den betroffenen Internetznutzern gerichtlichen Rechtsschutz ermöglichen muss (BGH GRUR 2016, 268 Rn. 57 – Störerhaftung des Access Providers).

Dieses Erfordernis ist vorliegend nicht gewahrt. Den betroffenen Internetnutzern stehen keine gerichtlichen Rechtsschutzmöglichkeiten gegen die Einrichtung der Sperre durch die Antragsgegnerin offen. In Bezug auf DNS-Sperren durch den Access Provider hat der BGH entschieden, dass diesem Erfordernis dadurch Rechnung getragen werden könne, dass die Internetnutzer ihre Rechte gegenüber dem Access Provider auf der Grundlage des zwischen ihnen bestehenden Vertragsverhältnis gerichtlich geltend machen können (BGH a.a.O.).

Vorliegend bestehen keine vertraglichen Ansprüche, die es den Nutzern der Antragsgegnerin ermöglichen würden, die DNS-Sperre gerichtlich überprüfen zu lassen.

1.3.4.1.2 DNS-Sperre nicht geeignet

DNS-Sperren stellen einen unverhältnismäßigen Eingriff in die Informationsfreiheit der Nutzer der Antragsgegnerin dar. EuGH und BGH verlangen insoweit, dass Sperrmaßnahmen streng zielorientiert sind, indem sie die Urheberrechtsverletzung beenden, ohne Internetnutzern die Möglichkeit zu nehmen, rechtmäßig Zugang zu Informationen zu erlangen (BGH GRUR 2016, 268 Rn. 53 – Störerhaftung des Access Providers). Diesen Anforderungen genügt die der Antragsgegnerin auferlegte DNS-Sperre nicht.

Zum einen begegnet schon die Geeignetheit der DNS-Sperre durch die Antragsgegnerin durchgreifenden Bedenken. Maßnahmen zur Unterbindung des unerlaubten Zugriffs auf Schutzgegenstände müssen die Rechtsverletzung zwar nicht völlig abstellen, aber zumindest den unerlaubten Zugriff verhindern oder zumindest erschweren und die Internetnutzer zuverlässig vom Zugriff abhalten (BGH a.a.O. Rn. 48). Eine DNS-Sperre durch die Antragstellerin genügt selbst diesen geringen Anforderungen nicht. Wie oben unter I.2.5. beschrieben, wird eine DNS-Abfrage nach erfolgter Sperrung durch die Antragsgegnerin durch einen alternativen DNS-Resolver beantwortet. Es kommt damit auf technische Umgehungsmöglichkeiten nicht an, da auf dem normalen Abrufweg über den Browser automatisch ein anderer rekursiver Resolver als der der Antragsgegnerin den Domainnamen auflöst.

Zum anderen ist die Sperrwirkung nicht hinreichend zielgerichtet, da sie über die geltend gemachte Rechtsverletzung an den Tonaufnahmen hinaus sämtliche Inhalte der beanstandeten Domain betrifft. Die Rechtsprechung hat zum Kriterium der Zielgerichtetheit unter dem Gesichtspunkt des „Overblockings", d.h. der Sperrung mitbetroffener, rechtmäßiger Informationen, entschieden, dass es auf das Gesamtverhältnis von rechtmäßigen zu rechtswidrigen Inhalten auf der gesperrten Website ankomme und zu fragen sei, ob es sich um eine nicht ins Gewicht fallende Größenordnung von legalen Inhalten handelt (vgl. etwa BGH a.a.O. Rn. 55). Das von der Antragstellerin vorgelegte Gutachten (Anlage AST 2) ist insoweit nicht aussagekräftig. Gegenstand des Gutachtens ist nicht das Verhältnis von rechtmäßigen zu rechtswidrigen Inhalten i.S.d. vorgenannten Rechtsprechung, sondern das Verhältnis geschützten Inhalten zu gemeinfreien oder unbekannten Werken (Anlage AST 2, S. 3). Ob es sich bei den geschützten Inhalten um Rechtsverletzungen handelt, beantwortet das Gutachten nicht. Hinzu kommt, wie oben unter 1.3.1.2 dargelegt, dass das Gutachten rechtmäßige Inhalte wie die Beiträge des Diskussionsforums bei der Stichprobe und ihrer Gewichtung außer Acht lässt und deshalb erheblichen methodischen Zweifeln begegnet.

Weiterhin mangelt es an der Zielgerichtetheit auch deshalb, weil die Antragsgegnerin nahezu willkürlich einen von Tausenden von Anbietern rekursiver Resolver, die allein in Deutschland betrieben werden, auswählte.

Schließlich kann der Dienst nie trennscharf DNS-Sperren nur für Nutzer in Deutschland umsetzen. Der Ausführung der Antragstellerin, dass eine weltweite Sperrung der Domain rechtlich unerheblich sei, kann nicht gefolgt werden.

Durch die weltweite Sperrwirkung besteht eine erhöhte Gefahr, dass der Zugang zu Informationen, der in anderen Jurisdiktionen rechtmäßig ist, verhindert wird. Unabhängig davon, ob die rechtsverletzenden Inhalte, die über die beanstandete Domain zugänglich sind, auch in den Rechtsordnungen der TRIPS-Mitgliedstaaten rechtswidrig sind, ist die Frage zu beurteilen, ob die jeweiligen Rechtsordnungen eine Inanspruchnahme der Antragsgegnerin zugelassen hätten. Gerichtliche Anordnungen gegen DNS-Resolver sind international bislang Einzelfälle geblieben (vgl. Schwemer, Copyright Content Moderation at Non-Content Layers, in: Rosati, Handbook of European Copyright Law (2021), S. 11). Die Inanspruchnahme von DNS-Resolvern ist in anderen Jurisdiktionen, etwa aus den oben skizzierten Verhältnis- und Subsidiaritätserwägungen unter anderen Rechtsordnungen nicht möglich. Selbst in der Schweiz, in der die Antragsgegnerin ihren Sitz hat, hätte die vorliegende Beschlussverfügung mit großer Wahrscheinlichkeit nicht erlassen werden können. Das Schweizer Bundesgericht hat entschieden, dass Access Provider nach Schweizer Recht mangels eigenem Tatbeitrag nicht zur Einrichtung von DNS-Sperren aufgrund von Urheberrechtsverletzungen in Anspruch genommen werden können (Bundesgericht, Urteil vom 4. Februar 2019, 4A_433/2018). Dies muss erst recht für DNS-Resolver gelten, deren Tatbeitrag noch geringer als der des Access Providers ist. Die weltweite Sperrwirkung kann also dazu führen, dass eine Rechtsfolge eintritt, die nach anderen Rechtsordnungen nicht vorgesehen oder, wie im Falle der Schweiz, ausdrücklich ausgeschlossen ist. Damit würde eine gerichtliche Anordnung in einer Rechtsordnung dazu führen, dass gesetzliche Regelungen einer anderen Rechtsordnung ausgehebelt werden. Dieses Ergebnis kann außerhalb internationaler Abkommen, mit der die Vertragsstaaten diese Rechtsfolge akzeptieren, nicht intendiert sein. Sperrverfügungen gegen

rechtsverletzende Websites müssen daher territorial auf den Bereich begrenzt sein, für den die Rechtsverletzung geltend gemacht wird.

Der Vortrag der Antragstellerin zur weltweiten Sperrwirkung (Antrag, S. 15) kann deren Zumutbarkeit nicht begründen. Die Antragstellerin verweist zunächst darauf, dass sich auch das Notice-and-Takedown-Verfahren weltweit auswirke. Dies ist nicht mit der Einrichtung einer DNS-Sperre vergleichbar. Denn das Notice-and-Takedown-Verfahren führt zur gezielten Entfernung eines einzelnen, rechtswidrigen Inhaltes, die Einrichtung einer DNS-Sperre zur Unerreichbarkeit einer gesamten Domain. Diese Verfahren sind rechtlich nicht vergleichbar und werden dementsprechend auch in der rechtswissenschaftlichen Literatur als gegensätzliche, nicht komplementäre Ansätze behandelt („löschen statt sperren", vgl. etwa MMR Aktuell, 303415).

Soweit die Antragstellerin sich auf die Entscheidung des EuGH in der Sache *Glawischnig-Piesczek ./. Facebook Ireland Ltd* beruft, ist klarzustellen, dass der EuGH lediglich geurteilt hat, dass die Richtlinie 2000/31/EG es einem Gericht nicht verwehrt, Sperrungsverfügungen mit internationaler Wirkung auszusprechen, *soweit dies nach internationalem Recht zulässig ist* (EuGH, Urt. v. 03.01.2019, C-18/18 - Glawischnig-Piesczek, Rn.51). Die Entscheidung beschränkt sich bezüglich der extraterritorialen Reichweite der Verfügungen mitgliedstaatlicher Gerichte auf die knappe Feststellung, die E-Commerce-RL sehe keine räumliche Beschränkung der Reichweite der Maßnahmen vor. Die Mitgliedstaaten müssen aber dafür Sorge tragen, dass die von ihnen erlassenen Maßnahmen mit internationalem Recht vereinbar sind (a.a.O. Rn. 52). Ob eine Verfügung mit extraterritorialer Wirkung nach internationalem Recht zulässig ist, muss demnach im Einzelfall erst festgestellt werden. Zur Zulässigkeit der Verfügung mit weltweiter Wirkung nach internationalem Recht trägt die Antragstellerin indes nicht vor.

Dass die Antragsgegnerin die beantragte Sperre nicht trennscharf für Deutschland umsetzen kann, führt dazu, dass diese Anordnung unverhältnismäßig ist. Die Antragstellerin hätte sich an die nationalen Access Provider wenden müssen, die aufgrund ihrer territorialen Marktbegrenzung und ihrer weitaus größeren Marktanteile als die Antragsgegnerin in der Lage sind, die Rechtsverletzung sowohl gezielter, als auch effektiver zu unterbinden.

1.3.4.2 Unverhältnismäßiger Eingriff in Berufsfreiheit der Antragsgegnerin

Die Verpflichtung zur Umsetzung der DNS-Sperre beeinträchtigt die Antragsgegnerin unverhältnismäßig in ihrem Recht auf unternehmerische Freiheit gem. Art. 16 GrCh und Art. 12 Abs. 1 GG. Nach der ständigen Rechtsprechung des BGH dürfen Diensteanbietern keine Maßnahmen auferlegt werden, die ihr Geschäftsmodell gefährden oder ihre Tätigkeit unverhältnismäßig erschweren (BGH GRUR 2007, 890 = NJW 2008, 758 – Jugendgefährdende Medien bei eBay). Im Rahmen der Grundrechtsabwägung ist daher auch der administrative, technische und finanzielle Aufwand zu berücksichtigen, den die Antragsgegnerin aufbringen muss, um die DNS-Sperre umzusetzen (BGH GRUR 2016, 268 Rn. 37 – Störerhaftung des Access Providers).

Bei der Antragsgegnerin ist im Ausgangspunkt zu berücksichtigen, dass diese ohne Gewinnerzielungsabsicht handelt und lediglich ein automatisch ablaufendes Verfahren zur Verfügung stellt, welches ihren Nutzern den Zugriff auf beanstandete Domain vermittelt. Ihr passiv neutraler automatischer Beitrag ist nicht vergleichbar mit dem eines Plattformbetreibers, wie er etwa den BGH-Entscheidungen zu Internetauktionshäusern zugrunde lag (so auch OLG Frankfurt a.M., Urteil v. 22.01.2008 - 6 W 10/08, GRUR-RR 2008, 93, 94 – Access-Provider, dort zu wettbewerbsrechtlichen Ansprüchen). Dort hat das Gericht bei der Frage der Zumutbarkeit von Pflichten darauf abstellen können, dass die Betreiber der Plattformen und Foren selbst die Gefahrenquellen für Rechtsverletzungen gesetzt haben, es ihnen gerade auch auf die Inhalte ankommt und dass dort ganz andere Möglichkeiten einer besseren Beeinflussung und Kontrolle der Inhalte bestand. Die Antragsgegnerin hat demgegenüber selbst keine neue Gefahrenquelle gesetzt und als neutraler technischer Vermittler mit den Inhalten, zu denen sie den Zugang vermittelt, nichts zu tun und keinerlei Einfluss darauf. Sie hat damit einen deutlich größeren Abstand zu den rechtsverletzenden Inhalten, wodurch auch die Zumutbarkeitsgrenzen eingeengt werden (vgl. OLG Hamburg, Urteil vom 22.12.2010 - 5 U 36/09).

Weiter muss berücksichtigt werden, dass die Antragsgegnerin ihren Dienst grundsätzlich global und einheitlich anbietet. Internetnutzer weltweit können den Dienst der Antragsgegnerin nutzen, indem sie in ihren Netzwerkeinstellungen als DNS-Resolver den Dienst Antragsgegnerin mit der IP-Adresse 9.9.9.9. konfigurieren. Dies unterscheidet die vorliegende Situation von Sperrverfügungen Access Provider, die den Gerichtsentscheidungen zur Störerhaftung des Access Providers zu Grunde liegt. Die DNS-Resolver der Access Provider verarbeiten nur Anfragen ihrer Vertragskunden. Access Provider können DNS-Sperren daher nur geografisch begrenzt umsetzen, da sie nur Anfragen aus dem Gebiet ihrer Vertragskunden verarbeiten. Das System der Antragsgegnerin sieht eine geografische Differenzierung zwischen den Anfragen der Nutzer nicht vor. Sie kann die DNS-Sperre nur umsetzen, in dem sie entweder mit erheblichem Aufwand durch manuelle kostenträchtige Konfiguration oder durch die Programmierung einer bisher nicht vorhandenen Funktionalität einrichtet, konfiguriert und unterhält, damit das System in der Lage ist, Sperrbefehle auf geografischer Basis umzusetzen. Wie bereits ausgeführt, handelt es sich bei der Antragsgegnerin um eine gemeinnützige Stiftung, die bislang keine Aufforderungen erhielt, DNS-Sperren für Urheberrechtsverletzungen einzusetzen. Allein die Kosten für die Einrichtung eines solchen Systems könnten für die Antragstellerin erdrosselnde Wirkung haben.

Die Einrichtung von DNS-Sperren führt zudem zu erheblichen Einbußen bei der Performanz des DNS-Resolvers der Antragsgegnerin. Diese Einbußen gefährden das Geschäftsmodell der Antragsgegnerin. Die Qualität eines DNS-Resolvers bemisst sich maßgeblich nach seiner Performanz, d.h. wie schnell der DNS-Resolver DNS-Anfragen auflöst. Die Qualität von DNS-Resolvern wird auf verschiedenen Internetportalen jeweils anhand der Performanz der Resolver, also der Geschwindigkeit der Beantwortung der Anfragen angegeben (vgl. etwa: https://www.dnsperf.com/#!dns-resolvers; hier werden DNS-Resolver gar nicht erst aufgeführt, wenn sie länger als eine Sekunde für die Auflösung einer Anfrage benötigen). Die Umsetzung der DNS-Sperre für Anfragen von Internetnutzern aus dem Gebiet der Bundesrepublik Deutschland führt für diese Nutzer zu einer spürbaren Verlangsamung des Dienstes der Antragsgegnerin (vgl. oben I.2.5.). Die Zuordnung der Anfragen zu einer bestimmten IP-

Adresse und deren geografische Zuordnung zum Gebiet der Bundesrepublik Deutschland ist mit erheblichem technischen Aufwand verbunden, da jede Anfrage an den Dienst der Antragsgegnerin darauf geprüft werden muss, ob die anfragenden IP-Adresse dem Gebiet der Bundesrepublik Deutschland zugeordnet werden kann und mit entsprechenden Sperrbefehlen beantwortet werden muss. Fällt die Performanz des Dienstes der Antragsgegnerin deutlich hinter die anderer öffentlicher DNS-Resolver zurück, ist damit zu rechnen, dass die Anfragenden einen anderen DNS-Resolver wählen werden. Dabei ist zu berücksichtigen, dass nur solche Internetnutzer den Dienst der Antragsgegnerin nutzen, die sich explizit dafür entscheiden, indem sie die Standard-Netzwerkeinstellungen ändern und an Stelle des voreingestellten DNS-Resolvers den der Antragsgegnerin eintragen. Diese Nutzer verfügen über das technische Verständnis und das Interesse an der Wahl eines bestimmten DNS-Resolvers, sodass sie einerseits in der Lage sind, einen alternativen DNS-Resolver in den Netzwerkeinstellungen zu konfigurieren und bei entsprechenden Einbußen der Performanz auf andererseits eine große Wahrscheinlichkeit besteht, dass sie auf einen anderen DNS-Resolver ausweichen werden.

Schließlich verfügt die Antragsgegnerin weder über das Budget noch über personelle oder fachliche Ressourcen, rechtliche Prüfungen zu beanstandeten Inhalten vorzunehmen. Dies gilt umso mehr, als dass der Dienst global erbracht wird. Daraus folgt, dass die Antragsgegnerin, die den Kreis der Anfragenden nicht wie andere Anbieter von Internetdiensten, die eine vertragliche Beziehung zu ihren Kunden eingehen, eingrenzen kann. Sie ist potenziell Prüfpflichten über Rechtsverletzungen aus den unterschiedlichsten Rechtsordnungen ausgesetzt. Es ist ihr faktisch unmöglich, Hinweisschreiben deren Substantiierung denen der von der Antragstellerin vorgelegten Schreiben entspricht, fundiert nachzugehen und zu prüfen. Dies gilt insbesondere dann, wenn wie das Gericht wie im vorliegenden Fall die wenig substantiierten Informationen, die von der Antragstellerin mitgeteilt wurden, weiterhin für ausreichend erachten würde.

Die Antragsgegnerin kann ihren Dienst nicht erbringen wenn – auch unter dem Aspekt bzw. der Gefahr der Verwirklichung von kerngleichen Verstößen – zukünftig eine Vielzahl von Sperraufforderungen auf sie zukommt. Diese kann die Antragsgegnerin aufgrund der fehlenden Mitarbeiterkapazitäten nicht prüfen und umsetzen. Setzt der Empfänger eine DNS-Sperre nicht um, da er die Faktenlage für zu dünn hält oder sie nicht nachvollziehen kann, so drohen kostenpflichtige Abmahnungen oder eine unter Umständen kostenträchtige und ressourcenintensive gerichtliche Auseinandersetzung. Es ist zu befürchten, dass viele (unabhängige und kleinere) Anbieter oder auch Unternehmen, die eigene rekursive Resolver betreiben, dieses Risiko nicht eingehen werden, sondern auch auf die Gefahr hin, rechtmäßige Inhalte zu sperren, eine DNS-Sperre ohne tiefergehende Prüfung der Berechtigung umsetzen werden.

Bevor die Antragsgegnerin der dauernden Gefahr der Verwirkung von Ordnungsmittelgeldern ausgesetzt ist, wird sie ihren Serverstandort in Europa aufgeben müssen. Dies wird nicht nur zu Lasten der Antragsgegnerin, sondern auch ihrer europäischen Nutzer gehen. Denn der Dienst der Antragsgegnerin wäre für Nutzer aus Deutschland auch bei einem Serverstandort außerhalb der EU weiterhin verfügbar, jedoch ohne dass die Einhaltung europäischer Datenschutznormen gewährleisten werden kann. Um Datenschutz und Datensicherheit bei

der Nutzung des DNS durch europäische Unternehmen zu fördern, hat die EU-Kommission die Initiative „DNS4EU“ (https://ec.europa.eu/digital-single-market/en/faq/faq-eu-cybersecurity-strategy-digital-decade) ins Leben gerufen, mit der die EU selbst einen europäischen DNS-Resolver einrichten wird, um die Einhaltung europäischer Datenschutzvorschriften zu ermöglichen und die Abhängigkeit der EU-Unternehmen von DNS-Resolvern in Drittstaaten zu verringern. Diese Bemühungen würden konterkariert, wenn die Antragsgegnerin ihren Dienst, der bereits jetzt den höchsten Datenschutzstandards genügt, einstellen müsste.

Die Beeinträchtigung der Antragsgegnerin in ihrer unternehmerischen Freiheit überwiegt bei der vorzunehmenden Abwägung die Beeinträchtigung der Antragstellerin in ihrem Eigentumsgrundrecht. Die Antragstellerin ist durch den Abruf der beanstandeten Domain über den Dienst der Antragsgegnerin nur unwesentlich in ihren rechtlichen Interessen berührt. Bei der Beurteilung der Schwere der Beeinträchtigung ist insoweit zu berücksichtigen, dass die Antragstellerin über die Empfehlung der CUII bereits DNS-Sperren der beanstandeten Domain bei sämtlichen großen deutschen Internetzugangsanbietern erwirkt hat. Für die weit überwiegende Mehrheit der Internetnutzer in Deutschland ist der Zugang zur beanstandeten Domain durch die Umsetzung der Empfehlung der CUII durch die beteiligten Access Provider bereits gesperrt. Der konkrete Abrufweg über den Dienst der Antragsgegnerin ist im Verhältnis der tatsächlichen Abrufe der beanstandeten Domain nur von untergeordneter Bedeutung. Die Nutzungsrate der Antragsgegnerin beträgt laut der Auswertung der APNIC am 30.08.2021 0,097% in Deutschland gegenüber 18,489% von Google.

Glaubhaftmachung: Screenshot statistische Auswertung der APNIC, abrufbar unter https://stats.labs.apnic.net/rvrs/QO?o=cXAw1l1s0t10x, als **Anlage AG 12**.

Würde es der Antragstellerin um die effektive Unterbindung des Zugangs zu der beanstandeten Domain gehen, müsste sie vorrangig andere DNS-Resolver mit größerem Marktanteil als die Antragsgegnerin, insbesondere den öffentlichen DNS-Resolver des Google-Konzerns, in Anspruch nehmen. In dieser Konstellation sind die Grundrechte der Betroffenen stärker zu Gunsten der Antragstellerin zu gewichten, da einer größeren Bedeutung des Abrufwegs eine geringere wirtschaftliche Beeinträchtigung gegenübersteht. Im vorliegenden Fall kann jedoch die geringe wirtschaftliche Bedeutung des Abrufwegs über den Dienst der Antragsgegnerin nicht die Gefährdung von deren Geschäftsmodell rechtfertigen.

1.4 Hilfsantrag unbegründet

Der hilfsweise geltend gemachte Anspruch gem. § 7 Abs. 4 TMG ist ebenfalls unbegründet. Die Anforderungen der Zumutbarkeit, Verhältnismäßigkeit und Subsidiarität sind in § 7 Abs. 4 TMG ausdrücklich normiert. Diese Anforderungen sind vorliegend nicht gewahrt, insoweit wird auf die Ausführungen zur Störerhaftung verwiesen.

2. Kein Verfügungsgrund

Es liegt schließlich auch kein Verfügungsgrund vor.

Dieser ist gegeben, wenn zur Abwendung einer Gefährdung der Gläubigerinteressen eine vorläufige Sicherung im Eilverfahren notwendig ist. Es müssen Umstände vorliegen, die nach dem objektiven Urteil eines vernünftigen Menschen befürchten lassen, dass die Verwirklichung des Individualanspruches durch bevorstehende Veränderung des bestehenden Zustandes gefährdet ist (vgl. Seiler in: Thomas/Putzo, ZPO, 39. Aufl. 2018, § 935 Rn. 6, § 940 Rn. 5 m.w.N.).

Auch wenn in diesem Bereich bestimmte Fristen nur als Anhaltspunkt dienen können, ist in der Regel von fehlender Dringlichkeit auszugehen, wenn der Unterlassungsgläubiger ohne zwingende Gründe einen Zeitraum von mehr als einem Monat ab Kenntnis der Rechtsverletzung bis zur Antragstellung verstreichen lässt (OLG Köln, Beschluss v. 22.01.2010 - 6 W 149/09, GRUR-RR 2010, 493 - Ausgelagerte Rechtsabteilung).

Nach diesen Grundsätzen ist der Antrag der Antragstellerin auf Erlass einer Verfügung nicht fristwahrend eingegangen. Die Antragstellerin hat die Monatsfrist verstreichen lassen. Die Antragstellerin hat selbst vorgetragen und durch eidesstattliche Versicherung [redacted] (Anlage AST 3) glaubhaft gemacht, dass sie Kenntnis von der Rechtsverletzung am 11.03.2021 erlangt hat. Der Antrag auf Erlass einer einstweiligen Verfügung datiert vom 12.04.2021, wurde mithin mehr als einen Monat nach Kenntniserlangung verfasst und ist erst am 14.04.2021 bei Gericht eingegangen.

Die Frage der Dringlichkeit ist nicht werkbezogen zu beurteilen (vgl. OLG München, Urteil v. 17.10.2019 - 29 U 1661/19, BeckRS 2019, 25462), weil es der Antragstellerin nicht um die Sperrung eines Werkes geht, sondern um die Sperrung einer DNS-Abfrage-Auflösung. Die konkret beantragte Maßnahme ist nicht auf ein bestimmtes Schutzrecht, sondern darauf gerichtet, dass der Zugang zu einer Domain insgesamt nicht mehr vermittelt wird und die Nutzer der Antragsgegnerin folglich auf sämtliche Inhalte der mit der Domain verknüpften Website nicht mehr zugreifen können. Ergibt sich der geltend gemachte Anspruch nicht allein aus der Verletzung eines konkreten Schutzrechts, sondern – wie vorliegend unter anderem aus dem Gesamtverhältnis rechtmäßiger und rechtswidriger Inhalte der beanstandeten Website – ist auch die Frage der Dringlichkeit nicht anhand des einzelnen Schutzrechts zu beurteilen (so auch BGH GRUR 2018, 1044 Rn. 27 – Dead Island zur der Frage, ob der prüfpflichtbegründende Hinweis für die Störerhaftung werkbezogen sein müsse). Der Antragstellerin ist seit längerem bekannt, dass über die beanstandete Website fortlaufend Urheberrechtsverletzungen an ihren Werken begangen werden. Die Antragstellerin hatte somit bereits zuvor die Möglichkeit, die Antragsgegnerin auf die beantragte DNS-Blockierung in Anspruch zu nehmen. Die Antragstellerin hielt mithin die Durchsetzung des von ihr geltend gemachten Anspruchs insgesamt nicht für dringlich. Eine selektive Wahrnehmung von Rechten aufgrund der Vermarktungsaktualität von Werken würde im Umkehrschluss keine dringliche Sperrung einer kompletten Domain rechtfertigen.

Davon abgesehen wurde auch unter Beachtung der Aktualität des Musikalbums die Monatsfrist nicht eingehalten.

Der Antrag auf Erlass einer einstweiligen Verfügung ist nach alledem unzulässig und unbegründet.

C. Streitwert

Der Unterlassungsstreitwert ist mit 100.000 EUR zu hoch angesetzt. Der Streitwert ist nach §§ 53 GKG, § 3 ZPO zu bestimmen. An den bislang zu Website-Sperren ergangenen Gerichtsentscheidungen lässt sich ablesen, dass es bei der Bemessung des Streitwerts maßgeblich auf die Zahl der Kläger, die Anzahl der geltend gemachten Rechtsverletzungen, die Marktbedeutung des Access Providers und die Bedeutung der gesperrten Website ankommt.

Ausgehend von den insgesamt 12 Tonaufnahmen, wäre in einem Hauptsacheverfahren vorliegend ein Streitwert von maximal 30.000 EUR angemessen. Das LG München I hat in einem Hauptsacheverfahren mit drei führenden Musiklabels als Klägern, die Rechte an drei Musikalben gegenüber einem führenden deutschen Access Provider geltend machten und die Sperre der im Bereich Musikfilesharing führenden Website goldesel.to beantragten, einen Streitwert von 150.000 EUR zu Grunde gelegt (LG München I, Urt. vom 7. Juni 2019, 37 O 2516/18). Der Leitentscheidung des BGH zur Störerhaftung des Access Providers lag ein Streitwert im Hauptsacheverfahren von 600.000 EUR zu Grunde (Streitwertbeschluss OLG Köln vom 09.12.2011, 6 U 192/11 sowie Vorinstanz LG Köln vom 12. Oktober 2011, 28 O 362/10). In diesem Verfahren machten vier Kläger Rechte an sechs Musikalben mit insgesamt 120 Titeln gegen einen bundesweit tätigen Access Provider gegen die führende Website goldesel.to geltend. Das OLG Köln legte in der Entscheidung zur Störerhaftung des Registrars (OLG Köln, Urt. vom 31. August 2018, 6 U 14/18) im Hauptsacheverfahren bei einem Sperranspruch, der sich auf 9 Domains der führenden Website „The Pirate Bay" bezog und in dem Rechte an einem mehrfach ausgezeichneten Spielfilm geltend gemacht wurden, einen Streitwert von 100.000 EUR zu Grunde.

Vor diesem Maßstab muss der Streitwert vorliegend geringer angesetzt werden. Legt man die Anzahl der Tonaufnahmen in den Entscheidungen des LG München I und des BGH zu Grunde, wäre vorliegend für eine Hauptsacheverfahren ein Streitwert zwischen 50.000 und 60.000 EUR angemessen. Streitwertmindernd muss vorliegend jedoch berücksichtigt werden, dass die wirtschaftliche Bedeutung des geltend gemachten Sperranspruchs vorliegend wegen weiterer Umstände geringer ist. Die beanstandete Website [redacted] weist einen deutlich geringeren Traffic als die in den vorgenannten Verfahren beanstandete Website goldesel.to auf (Zugriffe aus Deutschland auf goldesel.to im September 2020: 3,06 Mio., Zugriffe auf [redacted] in Deutschland im gleichen Zeitraum: ca. [redacted]), sodass daran gemessen auch die Zahl der Abrufe rechtswidriger Inhalte um ca. 1/3 und im gleichen Verhältnis auch die wirtschaftliche Bedeutung der geltend gemachten Rechtsverletzung geringer ist.

Glaubhaftmachung: Kopie Roundtable DNS-Sperren, Liste ausgewählter urheberrechtsverletzender Website zur Vorlage beim Bundeskartellamt, S. 8f., abrufbar unter: https://fragdenstaat.de/anfrage/clearingstelle-urheberrecht-im-internet-und-netzsperren-durch-internetzugangsanbieter-1/615725/anhang/2020-11-16Schreibenincl.Anlagen.pdf, als **Anlage AG 13.**

Zudem ist auch die Anzahl der Zugriffe auf die Website unter Nutzung des Dienstes der Antragsgegnerin wegen deren weitaus geringerer Marktbedeutung deutlich niedriger als über bundesweit tätige Access Provider (s.o. 1.3.3.4.3, der Anteil der Internetnutzer in Deutschland, die den Dienst der Antragsgegnerin benutzen, betrug am 30.08.2021 lediglich 0,097% und damit einen Bruchteil des Marktanteils großer Access Provider). Dementsprechend ist der Streitwert im einstweiligen Verfügungsverfahren auf maximal 20.000 EUR festzusetzen.

Rechtsanwaltsgesellschaft Rickert mbH
durch:

Thomas Rickert, Rechtsanwalt